Desktops and Applications in Horizon 8

VMware Horizon 2312

vmware
by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Desktops and Applications in Horizon 8

1

This guide describes how to set up Windows and Linux machines for use as remote desktops in a VMware Horizon 8 deployment. With the Horizon Agent software, you can create and provision pools of single-session desktops. You can also deploy pools of desktops and applications running on multi-session hosts such as Microsoft Remote Desktop Services (RDS).

Intended Audience

This information is intended for anyone who wants to create and provision desktop and application pools. The information is written for experienced Windows and Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Introduction to Virtual Desktops

2

With VMware Horizon 8, you can create desktop pools that include thousands of Windows or Linux virtual desktops. You can deploy desktops that run on virtual machines (VMs) deployed in a VMware vSphere environment or manage access to desktops that run on non-vSphere machines or physical machines. Create one VM as a golden image, and Horizon 8 can generate a pool of virtual desktops from that image. The golden image is also known as a base image.

Read the following topics next:

- Creating Desktop Pools in Horizon VMware Horizon 8
- Deploying Windows Applications that Run on Desktop Pools with VM Hosted Applications
- Creating Desktop Pools for Specific Types of Workers
- Features of Linux Desktops in VMware Horizon 8

Creating Desktop Pools in Horizon VMware Horizon 8

Horizon 8 uses desktop pools as its basis of centralized management. You create pools of virtual machines and select settings that give all the machines in a pool a common desktop definition. Horizon 8 can then deliver the desktops to end users through Horizon Clients.

You create a desktop pool from one of the following sources:

- A Windows or Linux virtual machine hosted on an ESXi host and managed by vCenter Server.
- A Windows virtual machine running on a virtualization platform other than vCenter Server that supports Horizon Agent.
- A physical Windows or Linux computer.
- A multi-session desktop on a multi-session host.
  - You can create a Windows multi-session desktop pool from an RDS host.
  - You can create a Linux multi-session desktop pool from a Linux host that supports mutli-session capabilities.

You can create the following types of desktop pools:

Desktop Pool Type	Description
Automated	Automated desktop pools use a vCenter Server virtual machine template or snapshot to create a pool of identical virtual machines. You can create these automated desktop pools: ■ Instant-clone desktop pools. ■ Full-clone virtual machine desktop pools.
Manual	Manual desktop pools are a collection of existing vCenter Server virtual machines, physical computers, or non-vCenter Windows virtual machines. For manual pools, Horizon 8 does not create and manage the life cycle of the desktops in the pool. The desktops are created outside of Horizon 8 and then imported into Horizon Console.

Deploying Windows Applications that Run on Desktop Pools with VM Hosted Applications

You can deliver one or multiple published Windows applications to end users without creating a farm of RDS hosts by creating a pool of virtual machine desktops to host the applications and then expose end users to only the published applications.

This approach benefits the following applications types:

- Applications that are only tested and certified on Windows 11 or 10.
- Applications that require .NET framework version compatibility.
- Applications that require special device support, where drivers may not run or be supported on RDS Hosts.
- Applications that require an install license and usage reporting by independent software vendors.

For more information, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at https://techzone.vmware.com.

Creating Desktop Pools for Specific Types of Workers

The most fundamental question to consider is whether a certain type of user needs a persistent desktop or a non-persistent desktop. Whether you use persistent or non-persistent desktops depends on the specific type of worker.

Persistent Desktop

Persistent desktops have data in the operating system image itself that must be preserved, maintained, and backed up. For example, users who need to install some of their own applications or have data that cannot be saved outside of the virtual machine itself (such as on a file server or in an application database) require a persistent desktop.

There are several ways to create persistent desktops in VMware Horizon 8:

- You can create pools of full clones (also known as full virtual machines).
- If you have already created virtual desktops or physical desktops (vCenter Server virtual machines, non-vCenter Server virtual machines, or physical machines), you can import them into Horizon 8 as persistent desktops using the dedicated-assignment manual desktop pool.

Persistent desktops give users the highest degree of flexibility and control over their own desktops. However, peersistent desktops consume more compute resources and are more difficult to manage by IT. These desktops might require traditional image management techniques.

Persistent desktops can have low storage costs in conjunction with certain storage system technologies. Since each persistent desktop is unique and must be preserved, backup and recovery technologies are important when considering strategies for business continuity.

Non-persistent Desktop

Non-persistent desktops are stateless images that are identical to one another. They are primarily used by users who do not need to install or preserve their own applications.

Non-persistent desktops have many advantages, such as being easier to support and having lower storage costs. Other benefits include a limited need to back up the virtual machines and easier, less expensive disaster recovery and business continuity options. The virtual desktops themselves do not need to be protected as there is no unique user data stored.

In the event that the virtual desktops are destroyed, you can simply re-create them from the golden image. Folder redirection and various profile technologies can optionally be used to storage user profile and user data. In Horizon 8 you can create non-persistent desktops by leveraging instant clones.

You can also specify how users are assigned desktops in a pool.

Dedicated-assignment pools	Each user is assigned a particular virtual desktop and returns to the same desktop at each login. Dedicated assignment pools require a one-to-one desktop-to-user relationship. For example, a pool of 100 desktops are needed for a group of 100 users.
Floating-assignment pools	Using floating-assignment pools also allows you to create a pool of desktops that can be used by shifts of users. For example, a pool of 100 desktops could be used by 300 users if they worked in shifts of 100 users at a time. The remote desktop is sometimes deleted and re-created after each use, offering a highly controlled environment.

Pools for Task Workers

Because task workers perform repetitive tasks within a small set of applications, you can utilize non-persistent desktops, which saves on storage an compute costs and make desktop management easier.

Use the following pool settings for instant-clone desktop pools:

- Use-floating assignment for the instant-clone desktop pool so that users log in to any available desktop. This setting reduces the number of desktops required if everyone does not need to be logged in at the same time.
- Configure the option to automatically logoff after disconnect, which deletes the instant clone whenever a user logs out. A new instant clone is created and ready for the next user to log in, thus effectively refreshing the desktop on every log out.
- To optimize compute resource utilization, use the dynamic pool provisioning capability of instant-clone desktop pools to grow or shrink the desktop pool based on demand. Be sure to specify enough spare desktops to satisfy the login rate.
- Consider storing instant-clone desktops on local ESXi data stores. This strategy can offer advantages such as utilizing inexpensive hardware, and faster virtual- machine provisioning. For a list of limitations for storing instant clones on local datastores, see Reducing Storage Requirements with Instant Clones.

  Note For information about other types of storage options, see Chapter 12 Managing Storage for Virtual Desktops.
- Use profile management tools such as VMware Dynamic Environment Manager or Microsoft FSLogix so that users always have their preferred desktop appearance and application settings with user profiles.

Pools for Knowledge Workers and Power Users

Knowledge workers usually are required to create complex documents and have them persist. Power users often need to install their own applications and have them persist. Depending on the nature and amount of personal data that must be retained, they require either a non-persistent desktop or a persistent desktop.

Use the following settings with non-persistent desktops for knowledge workers who do not need to install their own applications:

- Create dedicated-assignment desktop pools so that each user is guaranteed to have a virtual desktop anytime they login.
- Implement folder redirection, roaming profile, or another profile management solution to store and persist the user profile and user data.

For workers who must install their own applications, which adds data to the operating system disk, the best option is to create full-clone virtual machine desktops.

Pools for Kiosk Users

Kiosk users might include customers at airline check-in stations, students in classrooms or libraries, medical personnel at medical data entry workstations, or customers at self-service points. Accounts associated with client devices rather than users are entitled to use these desktop pools because users do not need to log in to use the client device or the remote desktop. Users can still be required to provide authentication credentials for some applications.

Virtual machine desktops that are set to run in kiosk mode use non-persistent desktops because user data does not need to be preserved in the operating system disk. Kiosk mode desktops are used with thin client devices or locked-down PCs. You must ensure that the desktop application implements authentication mechanisms for secure transactions, that the physical network is secure against tampering and snooping, and that all devices connected to the network are trusted.

As a best practice, use dedicated Horizon Connection Server instances to handle clients in kiosk mode, and create dedicated organizational units and groups in Active Directory for the accounts of these clients. This practice not only partitions these systems against unwarranted intrusion, but also makes it easier to configure and administer the clients.

To set up kiosk mode, you must use the `vdadmin` command-line interface and perform several procedures documented in the kiosk mode topics in the *Horizon 8 Administration* document.

As part of this setup, you can use the following instant-clone desktop pool settings.

- Use-floating assignment for the instant-clone desktop pool so that users log in to any available desktop. This setting reduces the number of desktops required if everyone does not need to be logged in at the same time.
- Configure the option to automatically logoff after disconnect, which deletes the instant clone whenever a user logs out. A new instant clone is created and ready for the next user to log in, thus effectively refreshing the desktop on every log out.

- Consider storing instant-clone desktops on local ESXi data stores. This strategy can offer advantages such as utilizing inexpensive hardware, and faster virtual- machine provisioning. For a list of limitations for storing instant clones on local datastores, see Reducing Storage Requirements with Instant Clones.

  Note For information about other types of storage options, see Chapter 12 Managing Storage for Virtual Desktops.

- For Windows desktop pools, use an Active Directory GPO (Group Policy Object) to configure location-based printing, so that the desktop uses the nearest printer. For a complete list and description of the settings available through the Group Policy Administrative templates (ADMX files), see the *Horizon Remote Desktop Features and GPOs* document.
- Use a GPO or Smart Policies to control whether local USB devices are connected to the desktop when the desktop is launched or when USB devices are plugged in to the client computer.

Features of Linux Desktops in VMware Horizon 8

The following list summarizes the key features supported on Linux desktops in a Horizon 8 environment.

Note Where applicable, the following entries identify the subset of Linux distributions that support a given feature. For the complete list of Linux distributions supported for Horizon Agent, see System Requirements for Horizon Agent for Linux.

Active Directory Integration

- OpenLDAP Pass-through Authentication supports integration with Active Directory for desktops running any Linux distribution supported by Horizon Agent.

  Note For OpenLDAP Pass-through Authentication, you can perform the configuration in a template virtual machine. No additional steps are required in the cloned virtual machines.

- System Security Services Daemon (SSSD) Authentication supports offline domain join with Active Directory for instant-cloned desktops running the following Linux distributions.
  - Ubuntu 20.04/22.04
  - Debian 10.x/11.x/12.x
  - RHEL 7.9/8.x/9.x
  - Rocky Linux 8.x/9.x
  - CentOS 7.9
  - SLED/SLES 15.x

- PowerBroker Identity Services Open (PBISO) Authentication supports offline domain join with Active Directory for instant-cloned desktops running the following Linux distributions.
  - Ubuntu 20.04/22.04
  - RHEL 7.9
- Samba supports offline domain join with Active Directory for instant-cloned desktops running any Linux distribution supported by Horizon Agent. However, VMware recommends using SSSD Authentication for desktops running newer distributions and Samba only for desktops running older distributions, as described in the following note.

  Note

  - VMware recommends using the SSSD Authentication method (instead of Samba) for desktops running the following Linux distributions.
    - Ubuntu 20.04/22.04
    - Debian 11.x/12.x
    - RHEL 8.x/9.x
    - Rocky Linux 8.x/9.x
    - SLED/SLES 15.x
  - VMware recommends using the Samba method for desktops running the following Linux distributions.
    - Debian 10.x
    - RHEL/CentOS 7.9

For more information, see the subtopics under Integrating Linux Desktops with Active Directory.

Application Pools

You can create single-session application pools that run on virtual Linux desktops. Each application in a single-session pool can support a single user session at a time.

You can create multi-session application pools based on manual or automated instant-clone farms of Linux host machines. Each application in a multi-session pool can support multiple user sessions at a time. For more information, see Creating Application Pools.

Audio-in and Audio-out

Linux desktops support audio input redirection from a client host as part of the Real-Time Audio-Video feature. See the entry for "Real-Time Audio-Video" in this article.

Audio input redirection is distinct from the USB redirection feature. You must select the system default audio in device "PulseAudio server (local)" in your application for the audio input.

Linux desktops support audio output redirection. This feature is enabled by default. To deactivate this feature, you must set the `RemoteDisplay.allowAudio` option to **`false`**. When accessed using Chrome and Firefox browsers, VMware Horizon HTML Access provides audio-out support for Linux desktops.

Note To enable audio input and audio output redirection on a RHEL 9.x, Rocky Linux 9.x, or Debian 12.x desktop, you must install the PulseAudio sound server on the source virtual machine, as described in the following procedure.

1 Install the PulseAudio packages.

- For RHEL or Rocky Linux 9.x:

```
sudo dnf install -y pulseaudio-module-x11 pulseaudio-utils
```

- For Debian 12.x:

```
sudo apt install -y pulseaudio pulseaudio-utils
```

2 Restart the machine.

Automated Full-Clone Desktop Pool

You can create automated full-clone desktop pools of single-session Linux desktops. For more information, see Chapter 8 Create and Manage Automated Full-Clone Desktop Pools.

Client Drive Redirection

When you enable the Client Drive Redirection (CDR) feature, your local system's shared folders and drives become available for you to access. Use the `tsclient` folder located in your home directory in the remote Linux desktop. To use this feature, you must install the CDR components.

Clipboard Redirection

With the clipboard redirection feature, you can copy and paste a rich text or a plain text between a client host and a remote Linux desktop. You can set the copy/paste direction and the maximum text size using Horizon Agent options. This feature is enabled by default. You can deactivate it during installation.

Desktop Environments

Horizon Agent for Linux supports multiple desktop environments on different Linux distributions. For more information, see the "Desktop Environment" section in System Requirements for Horizon Agent for Linux.

Desktop Pools

You can create single-session virtual desktops based on manual, automated full-clone, or automated instant-clone pools of Linux machines. Each virtual desktop can support a single user session at a time.

You can create multi-session published desktops based on manual or automated instant-clone farms of Linux host machines. Each published desktop can support multiple user sessions at a time. For more information, see Creating Published Desktop Pools.

Digital Watermark

You can create a unique digital watermark as a solution for authenticity, content integrity, and ownership protection of your intellectual property. A watermark shows traceable information that can deter people from potentially stealing your data.

The watermark can be displayed on the following Linux remote sessions:

- Multi-session applications and applications running on a desktop pool
- Virtual desktops and multi-session hosts
- Multiple monitors
- Primary session in a collaborative session

The watermark feature has the following limitations:

- Recorded sessions in Zoom or Webex applications do not include the watermark.
- Screen capture applications and the Print Screen key operated from within the remote desktop do not include the watermark. However, screen capture applications and the Print Screen key operated from the client system do include the watermark.
- If you use an old client version with the latest agent version, the watermark might not appear in the display.
- If you use the latest client version with an old agent version, the watermark does not appear in the display.
- A shadow session in a collaborative session cannot show the watermark.
- The watermark does not display when the **Search**, **Activities**, or **Show Applications** desktop features are in use.

You can configure the digital watermark using the following methods:

- Configuration options in the `/etc/vmware/config` file. See Edit Configuration Files on a Linux Desktop.
- Dynamic Environment Manager environment variables. See Set Up Digital Watermarks on a Linux Desktop With Environment Variables. The environment variable settings take priority over the settings in `/etc/vmware/config`.

Display Scaling

With the Display Scaling feature enabled, Linux remote desktops support the client display's scale factor. If the DPI (Dots Per Inch) setting on the remote desktop does not match the DPI setting on the client system, the remote session is displayed using a scale factor that matches the client system.

This feature is turned off by default. You can enable it by setting a configuration option as described in Edit Configuration Files on a Linux Desktop.

DPI Synchronization

The DPI Synchronization feature ensures that the DPI setting in a remote session changes to match the DPI setting of the client system when users connect to a Linux remote desktop or published application.

This feature is enabled by default. You can deactivate it by modifying a configuration option as described in Edit Configuration Files on a Linux Desktop.

FIPS 140-2 Mode

The Federal Information Processing Standard (FIPS) 140-2 mode, although not yet validated with the NIST Cryptographic Module Validation Program (CMVP), is available for Linux desktops running a RHEL 8.x distribution.

Horizon Agent for Linux implements cryptographic modules that meet FIPS 140-2 compliance. These modules were validated in operational environments listed in CMVP certificate #2839 and #2866, and were ported to this platform. However, the CAVP and CMVP testing requirement to include the new operational environments in VMware's NIST CAVP and CMVP certificates remains to be completed on the product roadmap.

Note To support FIPS 140-2 mode, you must use Transport Layer Security (TLS) protocol version 1.2.

For more information, see Configure a FIPS-compliant Linux Machine.

Help Desk Tool

Horizon Help Desk Tool is a Web application that you can use to troubleshoot Linux desktop sessions. You can use Horizon Help Desk Tool to get the status of user sessions and to perform troubleshooting and maintenance operations.

Horizon Recording

The VMware Horizon Recording feature allows administrators to record desktop and application sessions to monitor user behavior for Linux remote desktops and applications. For more information, see Using VMware Horizon Recording.

Horizon Smart Policies

You can use VMware Dynamic Environment Manager to create Smart Policies that control the behavior of the USB redirection, clipboard redirection, and client drive redirection features on specific remote Linux desktops. See Using Smart Policies.

Instant-clone Floating Desktop Pool

You can create instant-clone floating desktop pools of single-session Linux desktops.

For more information, see Chapter 7 Creating and Managing Instant-Clone Desktop Pools.

IPv6 Support

You can run Linux desktops and applications in an IPv6 environment. For a list of the Horizon 8 features supported in an IPv6 environment, see "Installing VMware Horizon 8 in an IPv6 or Mixed IPv4/IPv6 Environment" in the *Horizon 8 Installation and Upgrade* document.

To enable IPv6 support on a Linux machine, you must install Horizon Agent with the `--ipv6` optional parameter as described in Command-line Options for Installing Horizon Agent for Linux .

The `Subnet6` option in the `/etc/vmware/viewagent-custom.conf` configuration file lets you specify the IPv6 subnet of the Linux machine.

Keyboard Layout and Locale Synchronization

This feature specifies whether to synchronize a client's system locale and current keyboard layout with the Linux desktops. With the setting enabled or not configured, synchronization is allowed. With the setting deactivated, synchronization is not allowed.

Linux desktops support this feature only with Horizon Client for Windows, Mac, and Linux, and only for the English, French, German, Japanese, Korean, Spanish, Simplified Chinese and Traditional Chinese locales.

Lossless PNG

Images and videos generated on a desktop display on the client device in a pixel-exact manner.

Manual Desktop Pool

When configuring a manual desktop pool of single-session Linux desktops, you can select from the following options for machine source:

- Managed Virtual Machine - Machine source of the vCenter virtual machine. Both new and upgrade deployments support managed virtual machines.
- Unmanaged Virtual Machine - Machine source of other sources. An unmanaged virtual machine is only supported when the upgrade is from an unmanaged virtual machine deployment.

Note To ensure the best possible performance, do not use an unmanaged virtual machine.

Monitor Resolutions and Multiple Monitors

vGPU desktops support a maximum resolution of 3840x2160 on one, two, three, or four monitors configured in any arrangement.

2D desktops support the following maximum resolutions:

- 3840x2160 on a single monitor
- 2560x1600 on three monitors configured in any arrangement
- 2048x1536 on four monitors configured in any arrangement
- 2560x1600 on four monitors configured as follows:
  - Two monitors arranged on the bottom and two monitors arranged on the top
  - Four monitors stacked vertically on top of one another.

    The 2560x1600 resolution is not supported on four monitors arranged side by side.

Note To use the multiple monitors feature, verify that the desktop is running a supported desktop environment as described in Table 3-11. Supported Desktop Environments.

Network Intelligence Support for VMware Blast

VMware Blast supports the Network Intelligence transport. This feature is enabled by default.

When User Datagram Protocol (UDP) is enabled, Blast establishes both Transmission Control Protocol (TCP) and UDP connections. Based on the current network conditions, Blast dynamically selects one of the transports for transmitting data to provide the best user experience. For example, in a local area network, TCP performs better than UDP, so Blast selects TCP to transport data. Similarly, in a wide area network (WAN), UDP performance is better than TCP and Blast selects the UDP transport in that environment.

If one of the inline components used does not support UDP, Blast establishes a TCP connection only. For example, if your connection is using the Blast Security Gateway component of the Horizon Connection Server, Blast only establishes a TCP connection. Even if both client and agent enabled UDP, the connection uses TCP because Blast Security Gateway does not support UDP. If users are connecting from outside the corporate network, the UDP component requires VMware Unified Access Gateway, which supports UDP.

To establish a UDP-based Blast connection, follow these guidelines:

- If the client connects to a Linux desktop directly, enable UDP in both the client and agent. UDP is enabled by default in both the client and agent.
- If the client connects to a Linux desktop using Unified Access Gateway, enable UDP in the client, agent, and Unified Access Gateway.

Real-Time Audio-Video

Real-Time Audio-Video allows users to run Skype, Webex, Google Hangouts, Microsoft Teams, and other online conferencing applications in their remote sessions. With Real-Time Audio-Video, webcam and audio devices that are connected locally to the client system are redirected to the remote sessions.

This feature redirects video and audio data with a significantly lower bandwidth than can be achieved by using USB redirection. To enable Real-Time Audio-Video, you must install both the audio-in and webcam redirection features. For more information, see Install Real-Time Audio-Video on a Linux Machine.

Session Collaboration

With the Session Collaboration feature, users can invite other users to join an existing remote Linux desktop session, or you can join a collaborative session when you receive an invitation from another user. For more information, see Configuring Session Collaboration on Linux Desktops.

Single Sign-on

You can configure Active Directory single sign-on (SSO) for Linux desktops.

Smart Card Redirection and Smart Card SSO

Smart card redirection enables users to authenticate into Linux desktops using a smart card reader connected to the local client system. This feature is not supported on desktops running CentOS.

This feature supports Personal Identity Verification (PIV) cards and Common Access Cards (CAC). For more information, see Set Up Smart Card Redirection for Linux Desktops.

The smart card single sign-on (SSO) feature allows users to launch desktop sessions without entering their smart card credentials.

Screen-capture Blocking

With the screen-capture blocking feature enabled, users cannot take screenshots of their virtual desktop or published application from their endpoint using a Windows or macOS device. This feature is deactivated by default.

You can configure screen-capture blocking using the following methods:

- Configuration options in the `/etc/vmware/viewagent-custom.conf` file. See Edit Configuration Files on a Linux Desktop.
- Dynamic Environment Manager environment variables. See Configure Screen-Capture Blocking Using Environment Variables. The environment variable settings take priority over the settings in `/etc/vmware/viewagent-custom.conf`.

True SSO Support

You can configure the True SSO feature on Linux desktops.

For more information, see Set Up True SSO for Linux Desktops.

USB Redirection

The USB Redirection feature gives you access to locally attached USB devices from remote Linux desktops. You must install the USB Redirection components and USB VHCI driver kernel module to use the USB feature. Ensure that you have sufficient privileges to use the USB device that you want to redirect.

Video Codecs

Horizon Agent for Linux supports the following video compression methods, or codecs, for Blast Extreme. The agent machine must have the required hardware and drivers to support the codec.

- H.264
- High Efficiency Video Coding (HEVC)
- AOMedia Video 1 (AV1)

H.264 and HEVC can improve the Blast Extreme performance for a remote desktop, especially under a low-bandwidth network. HEVC provides higher image quality than H.264 at the same bandwidth.

If the client system has both H.264 and HEVC turned off, Blast Extreme automatically falls back to JPEG/PNG encoding.

The H.264 and HEVC encoders include both hardware support and software encoder support. The hardware support has the following requirements.

- The vGPU is configured with an NVIDIA graphics card. For more details, see the video codec support matrix on https://developer.nvidia.com.
- The NVIDIA driver 384 series or later is installed in the NVIDIA graphics card.

When the system meets the preceding requirements, Horizon Agent for Linux uses the hardware encoder. Otherwise, the software encoder is used.

VMware Integrated Printing

VMware Integrated Printing supports client printer redirection for Linux remote desktops. With client printer redirection, users can print from a Linux remote desktop to any local or network printer available on their client computer. VMware Integrated Printing with client printer redirection is enabled by default when you install Horizon Agent. For more information, see Configure VMware Integrated Printing for Linux Desktops.

VMware Integrated Printing also supports the ability to include a watermark with printed jobs. For more information, see Add Watermarks With VMware Integrated Printing on Linux Desktops.

VMware Integrated Printing is only supported on Linux desktops running RHEL 7.9/8.x/9.x, Rocky Linux 8.x/9.x, Ubuntu 20.04.x/22.04.x, or Debian 10.x/11.x/12.x.

3Dconnexion Mouse

To begin using your 3Dconnexion mouse, you must install the appropriate device driver and pair the mouse using the Connect USB Device menu on your Linux desktop.

3D Graphics

Horizon Agent for Linux supports vGPU graphics capabilities on systems configured with certain NVIDIA graphics cards and running certain operating systems.

Note For information about the NVIDIA graphics cards and Linux distributions that support vGPU capabilities, see https://docs.nvidia.com/grid/latest/product-support-matrix/index.html.

Limitations of Linux Desktops

Linux desktops have the following limitations:

- Location-based printing is not supported.
- The VMware HTML Access file transfer feature is not supported.
- Only the X11 display server protocol is supported. The Wayland protocol is not supported.

Additional limitations apply to multi-session published desktop pools and application pools. For more information, see Considerations for Linux Farms, Published Desktops, and Published Applications.

Creating and Preparing a Virtual Machine for Cloning

3

You can create a pool of desktop machines by cloning a vCenter Server virtual machine (VM). Before you create the desktop pool, you need to prepare and configure this VM, which is used as the base image to spawn cloned virtual desktops.

- For instant-clone desktop pools, the base image is called a **golden image**.
- For full-clone desktop pools, the base image is called a **Template Virtual Machine**.

This chapter is applicable if you are using VMware vSphere to create automated or manual desktop pools of virtual machines. For information about preparing non-vSphere machines for use in manual desktop pools, see Chapter 9 Creating and Managing Manual Desktop Pools.

For information about preparing machines for use as multi-session and Remote Desktop Services (RDS) hosts, see Chapter 15 Setting Up Published Desktops and Applications in Horizon.

Read the following topics next:

- Creating and Preparing a Windows Virtual Machine for Cloning
- Creating and Preparing a Linux Virtual Machine for Cloning
- Creating Virtual Machine Templates for Full-Clone Virtual Desktops
- Configure a Virtual Machine with Multiple NICs for Horizon Agent
- Using VMware Horizon Recording

Creating and Preparing a Windows Virtual Machine for Cloning

To create and prepare a VMware vSphere-based Windows virtual machine (VM) for use in an automated desktop pool, follow the documentation links on this page.

Creating a Windows Virtual Machine for Cloning

The first step in the process of deploying a pool of cloned desktops is to create a virtual machine in VMware vSphere and install and configure the operating system.

Procedure

1 Create a Windows Virtual Machine in VMware vSphere

You can create a Windows virtual machine (VM) in vSphere from scratch or by cloning an existing VM. This page describes creating a VM from scratch.

2 Create a Windows Virtual Machine with Virtualization-Based Security

You can create a virtual machine in VMware vSphere to use Virtualization-based security (VBS). Using a virtual machine enabled with VBS provides better protection from vulnerabilities within and malicious exploits to the operating system.

3 Install a Guest Windows Operating System

After you create a virtual machine, you must install a guest Windows operating system.

4 Prepare a Guest Windows Operating System for Remote Desktop Deployment

You must perform certain tasks to prepare a guest Windows operating system for remote desktop deployment.

5 Optimize Guest Windows Operating System Performance

You can use the operating system optimization tool to optimize guest Windows operating system performance for remote desktop deployment. While optimization is optional, taking some or all of the steps will improve your performance and VM consolidation significantly, leading to a lower cost-per-desktop.

6 Prepare Windows Server Operating Systems for Desktop Use

To use a supported Windows Server virtual machine as a single-session virtual desktop (rather than as an RDS host), you must perform certain steps before you install Horizon Agent in the virtual machine. You must also configure Horizon Console to treat Windows Servers as supported operating systems for VMware Horizon 8 desktop use.

7 Install Desktop Experience on Windows Server

For published desktops and applications, and for virtual desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Create a Windows Virtual Machine in VMware vSphere

You can create a Windows virtual machine (VM) in vSphere from scratch or by cloning an existing VM. This page describes creating a VM from scratch.

Prerequisites

Familiarize yourself with the custom configuration parameters for virtual machines. See Virtual Machine Custom Configuration Parameters.

Procedure

1 Log in to vSphere Client.

2 Right-click any inventory object that is a valid main object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**.

3 Select **Create a new virtual machine** and click **Next**.

4 Follow the prompts to specify the virtual machine custom options.

5 On the **Customize hardware** page, select **Virtual Hardware** to configure hardware settings.

   a Click **Add New Device** and select a CD/DVD drive, set the media type to use an ISO image file, select the ISO image file of an appropriate operating system, and select **Connect at power on**.

6 On the **Customize hardware** page, select **VM Options** to configure virtual machine settings.

   a **(Optional)** In the **Boot Options**, set **Boot Delay** to 10,000 milliseconds.

   You can set the boot delay to easily access the virtual machine's BIOS on boot and modify the system settings. After you modify the system settings, you can reboot the boot delay.

7 Click **Finish** to create the virtual machine.

8 Proceed to install the operating system.

Virtual Machine Custom Configuration Parameters

You can use virtual machine custom configuration parameters as baseline settings when you create a virtual machine for remote desktop deployment.

Table 3-1. Custom Configuration Parameters

Parameter	Description and Recommendations
`Name and Folder`	The name and location of the virtual machine. If you plan to use the virtual machine as a template, assign a generic name. The location can be any folder within your datacenter inventory.
`Host/Cluster`	The ESXi server or cluster of server resources that will run the virtual machine. If you plan to use the virtual machine as a template, the location of the initial virtual machine does not necessarily specify where future virtual machines created from template will reside.
`Resource Pool`	If the physical ESXi server resources are divided into resource pools, you can assign them to the virtual machine.
`Datastore`	The location of files associated with the virtual machine.

Table 3-1. Custom Configuration Parameters (continued)

Parameter	Description and Recommendations
`Hardware Machine Version`	The hardware machine version that is available depends on the ESXi version you are running. As a best practice, select the latest available hardware machine version, which provides the greatest virtual machine functionality. Certain VMware Horizon 8 features require minimum hardware machine versions.
`Guest Operating System`	The type of operating system that you will install in the virtual machine.
`CPUs`	The number of virtual processors in the virtual machine.
`Memory`	The amount of memory to allocate to the virtual machine.
`Network`	The number of virtual network adapters (NICs) in the virtual machine. One NIC is usually sufficient. The network name should be consistent across virtual infrastructures. An incorrect network name in a template can cause failures during the instance customization phases. When you install Horizon Agent on a virtual machine that has more than one NIC, you must configure the subnet that Horizon Agent uses. See Configure a Virtual Machine with Multiple NICs for Horizon Agent for more information. **Important** For Windows, you must use the VMXNET 3 network adapter.
`SCSI Controller`	The type of SCSI adapter to use with the virtual machine. Select either LSI Logic SAS or VMware Paravirtual (PVSCSI). Using PVSCSI may require additional steps depending on the version of Windows to be installed. For more information, see the VMware Knowledge Base article Configuring disks to use VMware Paravirtual SCSI (PVSCSI) controllers (1010398).
`Select a Disk`	The disk to use with the virtual machine. Create a new virtual disk based on the amount of local storage that you decide to allocate to each user. Allow enough storage space for the OS installation, patches, and locally installed applications. To reduce the need for disk space and management of local data, you should store the user's information, profile, and documents on network shares rather than on a local disk.

Create a Windows Virtual Machine with Virtualization-Based Security

You can create a virtual machine in VMware vSphere to use Virtualization-based security (VBS). Using a virtual machine enabled with VBS provides better protection from vulnerabilities within and malicious exploits to the operating system.

Prerequisites

- Microsoft Windows 10 (64-bit) or Windows Server 2016 (64-bit) or later operating system.
- Familiarize yourself with the custom configuration parameters for virtual machines. See Virtual Machine Custom Configuration Parameters.

Note VBS is not supported for vGPU-enabled virtual machines. URL Content Redirection and scanner redirection might not work properly with VBS enabled.

Procedure

1. Log in to vSphere Client.
2. Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**.
3. Select **Create a new virtual machine** and click **Next**.
4. Follow the prompts to specify the virtual machine custom options.
5. On the **Select a guest OS** page, select Windows as the guest OS and select Microsoft Windows 10 (64-bit) as the guest OS version. Then, select **Enable Windows Virtualization Based Security**.
6. To deploy automated desktop pools that contain full virtual machines or instant clones, on the **Customize hardware** page, verify that you do not add any Trusted Platform Module (vTPM) device. Connection Server adds a vTPM device to each virtual machine during the desktop pool creation process.
7. Follow the prompts to complete the virtual machine setup and click **Finish** to create the virtual machine.

What to do next

- Install the Windows 10 (64-bit) or Windows Server 2016 (64-bit) or later operating system on the virtual machine.
- On Windows 10, enable the VBS group policy. For more information, consult the article "Enable virtualization-based protection of code integrity" in the Microsoft documentation. Then reboot the virtual machine.
- On Windows Server 2016 and later builds, enable the VBS group policy, install the **Hyper-V** role and reboot the virtual machine.

Install a Guest Windows Operating System

After you create a virtual machine, you must install a guest Windows operating system.

Prerequisites

- For the list of supported guest Windows operating systems, see the VMware Knowledge Base (KB) articles https://kb.vmware.com/s/article/78714 and https://kb.vmware.com/s/article/78715.
- Verify that an ISO image file of the guest operating system is on a datastore on your ESXi server.
- Verify that the CD/DVD drive in the virtual machine points to the ISO image file of the guest operating system and that the CD/DVD drive is configured to connect at power on.

Procedure

1. In vSphere Client, log in to the vCenter Server system where the virtual machine resides.

2 Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

   Because you configured the CD/DVD drive to point to the ISO image of the guest operating system and to connect at power on, the guest operating system installation process begins automatically.

3 Click the **Console** tab and follow the installation instructions provided by the operating system vendor.

4 Activate Windows.

What to do next

Prepare the guest operating system for VMware Horizon 8 desktop deployment.

Prepare a Guest Windows Operating System for Remote Desktop Deployment

You must perform certain tasks to prepare a guest Windows operating system for remote desktop deployment.

Prerequisites

- Create a virtual machine and install a guest Windows operating system.
- Configure an Active Directory domain controller for your remote desktops. See the *Horizon 8 Installation and Upgrade* document for more information.
- To make sure that desktop users are added to the local Remote Desktop Users group of the virtual machine, create a restricted Remote Desktop Users group in Active Directory. See the *Horizon 8 Installation and Upgrade* document for more information.
- Verify that Remote Desktop Services are started on the virtual machine. Remote Desktop Services are required for Horizon Agent installation, SSO, and other VMware Horizon 8 operations. You can turn off RDP access to your Horizon 8 desktops by configuring desktop pool settings and group policy settings. See Prevent Access to VMware Horizon 8 Desktops Through RDP.
- Verify that you have administrative rights on the guest operating system.
- On Windows Server operating systems, prepare the operating system for desktop use. See Prepare Windows Server Operating Systems for Desktop Use.
- If you intend to configure 3D graphics rendering for desktop pools, familiarize yourself with the **Enable 3D Support** setting for virtual machines. On ESXi hosts, you can select options that determine how the 3D renderer is managed on the ESXi host. For details, see the *vSphere Virtual Machine Administration* document in the vSphere documentation.

Procedure

1 In vSphere Client, log in to the vCenter Server system where the virtual machine resides.

2 Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

3 Right-click the virtual machine, select **Guest**, and select **Install/Upgrade VMware Tools** to install the latest version of VMware Tools.

Note If you are using VMTools v11.x, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/78434.

4 Ensure that the virtual machine is synchronized to a reliable time source.

In general, guests can use the VMware Tools time synchronization method in preference to other methods of time synchronization. The VMware Tools online help provides information on configuring time synchronization between guest and host.

A Windows guest that is a member of a Windows domain synchronizes its time with its domain controller using the Windows Time Service. For these guests, this is the appropriate time synchronization method and VMware Tools time synchronization must not be used.

Guests must use only one method of time synchronization. For example, a Windows guest that is not a member of a Windows domain must have its Windows Time Service disabled.

Important Hosts that are being relied upon for time synchronization must themselves be synchronized to a reliable time source, using the built-in NTP client. Verify that all hosts in a cluster use the same time source.

Note Windows domain controllers can use either VMware Tools time synchronization or another reliable time source. All domain controllers within a forest and domain controllers across forests with inter-forest trusts must be configured to use the same time source.

5 Install service packs and updates.

6 Install antivirus software.

7 Install other applications and software, such as smart card drivers if you are using smart card authentication.

If you plan to use VMware Workspace ONE Access to offer a catalog that includes ThinApp applications, you must install Workspace ONE Intelligent Hub for Windows.

Important If you are installing Microsoft .NET Framework, you must install it after you install Horizon Agent.

8 If Horizon Client devices will connect to the virtual machine with the PCoIP display protocol, set the power option **Turn off the display** to **Never**.

If you do not disable this setting, the display will appear to freeze in its last state when power savings mode starts.

9 If Horizon Client devices will connect to the virtual machine with the PCoIP display protocol, go to **Control Panel > System > Advanced System Settings > Performance Settings** and change the setting for **Visual Effects** to **Adjust for best performance**.

   If you instead use the setting called **Adjust for best appearance** or **Let Windows choose what's best for my computer** and Windows chooses appearance instead of performance, performance is negatively affected.

10 If a proxy server is used in your network environment, configure network proxy settings.

11 Configure network connection properties.

   a Assign a static IP address or specify that an IP address is assigned by a DHCP server.

      Horizon 8 does not support link-local (169.254.x.x) addresses for Horizon 8 desktops.

   b Set the preferred and alternate DNS server addresses to your Active Directory server address.

12 (Optional) Join the virtual machine to the Active Directory domain for your remote desktops.

   A golden image virtual machine for creating instant clones must either belong to the same Active Directory domain as the domain that the desktop machines will join or be a member of a workgroup.

13 Configure Windows Firewall to allow Remote Desktop connections to the virtual machine.

14 (Optional) Deactivate Hot Plug PCI devices.

   This step prevents users from accidentally disconnecting the virtual network device (vNIC) from the virtual machine.

15 (Optional) Configure user customization scripts.

Optimize Guest Windows Operating System Performance

You can use the operating system optimization tool to optimize guest Windows operating system performance for remote desktop deployment. While optimization is optional, taking some or all of the steps will improve your performance and VM consolidation significantly, leading to a lower cost-per-desktop.

For instructions on how to use the operating system optimization tool, see Windows OS Optimization Tool for VMware Horizon Guide.

For more information on creating optimized Windows images, see Manually Creating Optimized Windows Images for VMware Horizon VMs or Using Automation to Create Optimized Windows Images for VMware Horizon VMs in the VMware Digital Workspace Tech Zone.

Prepare Windows Server Operating Systems for Desktop Use

To use a supported Windows Server virtual machine as a single-session virtual desktop (rather than as an RDS host), you must perform certain steps before you install Horizon Agent in the virtual machine. You must also configure Horizon Console to treat Windows Servers as supported operating systems for VMware Horizon 8 desktop use.

Prerequisites

- Familiarize yourself with the steps to install the Desktop Experience feature on Windows Server. See Install Desktop Experience on Windows Server.
- On Windows Server machines, familiarize yourself with the steps to configure the Windows Firewall service to restart after failures occur.

Procedure

1 Verify that the Remote Desktop Services role is not installed.

When the Remote Desktop Services role is not present, the Horizon Agent installer prompts you to install Horizon Agent in RDS mode or desktop mode. If the Remote Desktop Services role is present, the Horizon Agent installer does not display these options and it treats the Windows Server machine as an RDS host instead of a single-session Horizon 8 desktop.

2 During Horizon Agent installation, select **Desktop mode** to install Horizon Agent as a single-user virtual desktop where published desktop features will not be available.

3 (Optional) Install the Desktop Experience feature if you plan to use the following features.

- HTML Access
- Scanner redirection
- Windows Aero

4 (Optional) To use Windows Aero on a Windows Server desktop, start the Themes service.

When you create or edit a desktop pool, you can configure 3D graphics rendering for your desktops. The 3D Renderer setting offers a Software option that enables users to run Windows Aero on the desktops in the pool.

5 On Windows Server machines, configure the Windows Firewall service to restart after failures occur.

6 Configure Horizon Console to treat Windows Servers as supported desktop operating systems.

If you do not perform this step, you cannot select Windows Server machines for desktop use in Horizon Console.

a In Horizon Console, select **Settings > Global Settings**.

b In the **General Settings** tab, click **Edit**.

c Select the **Enable Windows Server desktops** check box and click **OK**.

Results

When you enable Windows Server desktops in Horizon Console, Horizon Console displays all available Windows Server machines, including machines on which Connection Server is installed, as potential machines for desktop use. You cannot install Horizon Agent on machines on which other Horizon 8 software components are installed.

Install Desktop Experience on Windows Server

For published desktops and applications, and for virtual desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Windows Server operating systems are supported on machines that are used as RDS hosts and on single-user virtual machines.

Note A Windows Server 2016 or later installation with the Desktop Experience option, installs the standard user interface and all tools, including the client experience and the desktop experience features. For Windows Server 2016 or later installation, select **Windows Server 2016** or **Windows Server 2019** or **Windows Server (Server with Desktop Experience)**. If you do not make a choice in the Setup wizard, Windows Server 2016 or Windows Server 2019 is installed as the Server Core installation option. You cannot switch between the installation options. If you install **Windows Server (Server with Desktop Experience)**, and later decide to use **Windows Server 2016** or **Windows Server 2019**, you must perform a fresh installation of Windows Server 2016 or Windows Server 2019.

Procedure

1 Log in as an administrator.

2 Start Server Manager.

3 Select **Add roles and features**.

4 On the Select Installation Type page, select **Role-based or feature-based installation**.

5 On the Select Destination Server page, select a server.

6 On the Select Server Roles page, accept the default selection and click **Next**.

7 On the Select Features page, under **User Interfaces and Infrastructure**, select **Desktop Experience**.

8 Follow the prompts and finish the installation.

Install Horizon Agent on a Windows Virtual Machine

You must install Horizon Agent on Windows virtual machines that are managed by vCenter Server so that Connection Server can communicate with them. Install Horizon Agent on all virtual machines that you use as templates for full-clone desktop pools and golden images for instant-clone desktops.

To install Horizon Agent on multiple Windows virtual machines without having to respond to wizard prompts, you can install Horizon Agent silently.

The Horizon Agent software cannot coexist on the same virtual or physical machine with other Horizon software components, including Connection Server. It can coexist with Horizon Client.

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon 8 Installation and Upgrade* document.
- Prepare the guest operating system for remote desktop deployment. See Prepare a Guest Windows Operating System for Remote Desktop Deployment.
- To use a Windows Server virtual machine as a single-session virtual desktop (rather than as an RDS host), perform the steps described in Prepare Windows Server Operating Systems for Desktop Use. To use a Windows Server virtual machine as an RDS host, see Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.
- Verify that you have administrative rights on the virtual machine.
- Familiarize yourself with the Horizon Agent custom setup options. See Custom Setup Options for Horizon Agent for Windows .
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *Horizon Overview and Deployment Planning* document for more information.
- Verify that you have a minimum of 2 CPUs to install or upgrade Horizon Agent from versions 7.x or later.

Procedure

1 To start the Horizon Agent installation program, double-click the installer file.

   The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

2 Accept the VMware license terms.

3 If you install Horizon Agent on a Windows Server machine on which the Remote Desktop Session Host (RDSH) role is not installed, the Horizon Agent installer prompts you to install Horizon Agent in RDS mode or Desktop mode. If the RDSH role is already installed on the system, by default the Horizon Agent installer will install Horizon Agent in RDS mode.

   - If you select **RDS mode**, the installer will install the Remote Desktop Session Host (RDSH) role and/or the Desktop Experience role and prompt you to restart the system. After the roles are installed and the system is restarted, launch the installer again to continue installing Horizon Agent in RDS mode.

- If you select **Desktop mode**, the installer will install Horizon Agent as a single-user virtual desktop where published desktop features will not be available.

4 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

You must install all Horizon 8 components with the same IP version.

5 Select whether to enable or disable FIPS mode.

This option is available only if FIPS mode is enabled in Windows.

6 Select your custom setup options.

By default, **VMware Horizon Instant Clone Agent** is enabled.

7 Accept or change the destination folder.

8 Follow the prompts in the Horizon Agent installation program and finish the installation.

Note If you did not enable Remote Desktop support during guest operating system preparation, the Horizon Agent installation program prompts you to enable it. If you do not enable Remote Desktop support during Horizon Agent installation, you must enable it manually after the installation is finished.

9 If you selected the USB redirection option, restart the virtual machine to enable USB support.

In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the virtual machine.

What to do next

If the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See Configure a Virtual Machine with Multiple NICs for Horizon Agent.

Custom Setup Options for Horizon Agent for Windows

When you install Horizon Agent, certain features are automatically installed on all guest Windows operating systems on which they are supported. In addition, you can select or deselect custom setup options.

To learn which features are supported on which guest operating systems, see "Feature Support Matrix for Horizon Agent" in the *Horizon Overview and Deployment Planning* document.

To change custom setup options after you install the latest Horizon Agent version, you must uninstall and reinstall Horizon Agent. For patches and upgrades, you can run the new Horizon Agent installer and select a new set of options without uninstalling the previous version.

In an IPv6 environment, VMware Audio options are selected and installed by default.

Table 3-2. Horizon Agent Features That Are Installed Automatically

Feature	Description
Core	Installs the core functionality.
PCoIP Agent	Lets users use the PCoIP display protocol to connect to the remote desktop. Installing the PCoIP Agent feature disables sleep mode on Windows desktops. When a user navigates to the Power Options or Shut Down menu, sleep mode or standby mode is inactive. Desktops do not go into sleep or standby mode after a default period of inactivity. Desktops remain in active mode.
PSG Agent	Installs the PCoIP Secure Gateway on remote desktops to implement the PCoIP display protocol.
VMware Blast	Installs the VMware Blast display protocol on remote desktops.
Windows Media Multimedia Redirection (MMR)	Extends multimedia redirection to Windows desktops and clients. This feature delivers a multimedia stream directly to the client computer, allowing the multimedia stream to be processed on the client hardware instead of the remote ESXi host.
HTML5 Multimedia Redirection	Redirects HTML5 multimedia content in a Chrome or Edge browser to the client, for performance optimization.
Browser Redirection	Renders a website on the client system instead of the agent system, and displays the website over the remote browser's viewport, when a user uses the Chrome browser in a remote desktop.
Media Optimization for Microsoft Teams	Redirects Microsoft Teams audio calls, video calls, and desktop share views to process on the client machine instead of in the virtual desktop.
Virtual video driver	Provides a virtual video driver on the remote desktop.
Unity Touch	Allows tablet and smart phone users to interact easily with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications, all without using the Start menu or Taskbar.
VMware Integrated Printing	Enables users to print to any printer available on their client machines. Location-based printing is supported. VMware Integrated Printing is supported on the following remote desktops and applications: ■ Desktops that are deployed on single-user machines, including Windows desktop and Windows server machines ■ Published desktops and published applications that are deployed on RDS hosts, where the RDS hosts are virtual machines or physical machines
vRealize Operations Desktop Agent	This feature that allows vRealize Operations Manager to monitor remote desktops is deprecated in this release. When you perform a fresh installation, the desktop agent will not collect data. When you perform an upgrade, if the desktop agent has been configured with vRealize Operations before the upgrade, the desktop agent will still collect and report data to vROps. You need to stop the service manually.

Table 3-3. Horizon Agent Custom Setup Options in an IPv4 Environment

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops. This option is not selected by default. You must select the option to install it. For guidance about using USB redirection securely, see the *Horizon Security* document. For example, you can use group policy settings to disable USB redirection for specific users. For information about using the USB redirection feature, and USB device type limitations, see "Using USB Devices with Remote Desktops and Applications" in the *Horizon Remote Desktop Features and GPOs* document.
Real-Time Audio-Video	Redirects webcam and audio devices that are connected to the client system so that they can be used on the remote desktop.
Client Drive Redirection	Allows Horizon Client users to share local drives with their remote desktops. After this option is installed, no further configuration is required on the remote desktop. Client Drive Redirection is also supported on published desktops and published applications and on virtual desktops that run on unmanaged machines.
Help Desk Plugin for Horizon Agent	You must have a Horizon Enterprise edition license or Horizon Apps Advanced edition license for Horizon to use the Help Desk Tool. This option is installed and enabled by default.
Scanner Redirection	Redirects scanning and imaging devices that are connected to the client system so that they can be used on the remote desktop or application. This option is not selected by default. You must select the option to install it.
Smartcard Redirection	Lets users authenticate with smart cards when they use the PCoIP or VMware Blast display protocol. This option is not selected by default. Smartcard Redirection is supported on remote desktops that are deployed on single-user machines.
Serial Port Redirection	Redirects serial COM ports that are connected to the client system so that they can be used on the remote desktop. This option is not selected by default. You must select the option to install it.
VMware Audio	Provides a virtual audio driver on the remote desktop.
UNC Path Redirection	Redirects UNC Path in Outlook 2013, 2016, 2019, 2021 or Office365 Outlook from agent-to-client, for performance optimization.
URL Content Redirection	Redirects URL content in an Internet Explorer 9, 10, or 11 browser, Chrome, Edge-chromium, Firefox, and third-party not-browser application from agent-to-client, for performance optimization.
VMware Horizon Instant Clone Agent	Lets this virtual machine be the golden image of an instant-clone desktop pool. This option is selected by default.
Fingerprint Scanner Redirection	Redirects fingerprint scanner devices that are plugged into a serial port on a Windows client system to virtual desktops, published desktops, and published applications.
Horizon Performance Tracker	Monitors the performance of the display protocol and system resource usage. This option is not selected by default. You must select the option to install it. .NET Framework 4.6.2 or later is required if you install Horizon Performance Tracker.

Table 3-3. Horizon Agent Custom Setup Options in an IPv4 Environment (continued)

Option	Description
SDO Sensor Redirection	Enables the Simple Device Orientation (SDO) sensor redirection feature. This option is not selected by default. You must select the option to install it.
Geolocation Redirection	Enables the Geolocation Redirection feature. This option is not selected by default. You must select this option to install it.

Modify Installed Components with theHorizon Agent for Windows Installer

The Horizon Agent for Windows installer allows you to modify already installed components without needing to uninstall and reinstall Horizon Agent.

You can run the Horizon Agent installer on a virtual machine where Horizon Agent is already installed to modify, repair, or remove previously installed components. You can also change custom setup options silently using the command line.

Note You cannot switch between installation types, such as managed to unmanaged machines. You also cannot modify Instant Clone Agent (NGVC).

Procedure

1 To start the Horizon Agent installation program, double-click the installer file. The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

  You can also use the **Uninstall or change a program** in the Control Panel: Click **VMware Horizon Agent**, then click **Change**.

2 Select **Modify** from these three options:

  - Modify: add or remove the components that are installed.
  - Repair: fix missing or corrupt files, shortcuts, and registry entries.
  - Remove: remove Horizon Agent from the computer.

3 Select or deselect features to add or remove them from the list.

4 Follow the prompts to finish the installation.

5 Restart the system for the changes to take effect.

What to do next

You can confirm the components that were removed (Absent) or added (Local) in the registry located at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\Installer\Features_HorizonAgent`.

Install a Horizon Agent for Windows Patch

You can install a Horizon Agent hotpatch on a Windows machine where Horizon Agent is already installed without needing to uninstall and reinstall Horizon Agent. You can also install a patch silently.

You can install the latest patch which is included in a Horizon Agent build.

Prerequisites

- In **Control Panel > Programs > Programs and Features** , verify Horizon Agent is already installed and note the build number.
- In **Control Panel > Programs > Programs and Features > Installed Updates**, verify the Horizon Agent Update Patch is the same build number as the Horizon Agent build.

Procedure

1. To start the Horizon Agent installation program, double-click the Horizon Agent Update Patch installer file. The installer filename is `VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.msp`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.
2. Select **Repair** from these three options:
   - Modify: add or remove the components that are installed.
   - Repair: install patches, fix missing or corrupt files, shortcuts, and registry entries.
   - Remove: remove Horizon Agent from the computer.
3. Follow the prompts to finish the installation.
4. Restart the system for the changes to take effect.

What to do next

Verify the patch build number is updated in the registry: `HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent` and `HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber` and in **Control Panel > Programs > Programs and Features > Installed Updates > Patch update version**.

Uninstall a Horizon Agent for Windows Patch

You can remove a Horizon Agent hotpatch from a Windows machine where Horizon Agent is already installed without needing to uninstall and reinstall Horizon Agent. You can also uninstall a patch silently by running a PowerShell script.

Prerequisites

- In **Control Panel > Programs > Programs and Features** , verify Horizon Agent is already installed and note the build number.

- In **Control Panel > Programs > Programs and Features > Installed Updates**, verify the Horizon Agent Update Patch is the same build number as the Horizon Agent build.

Procedure

1. To uninstall the patch, go to **Control Panel > Programs > Uninstall or change a Program** , select the patch and click **Uninstall**.

   Uninstalling a patch will revert to the previous build.

2. Restart the system for the changes to take effect.

What to do next

Verify that no reference of the patch exists in the registry: `HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent` and `HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber` or in **Control Panel > Programs > Programs and Features** .

Installing Horizon Agent for Windows Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install Horizon Agent on several Windows virtual machines or physical computers. In a silent installation, you do not have to respond to wizard prompts. A silent upgrade uses the same install commands. You can also modify already installed Horizon Agent components silently.

You can perform a silent installation either by entering parameters manually on the command line or by using a settings file.

About Silent Installation

With silent installation, you can efficiently deploy Horizon 8 components in a large enterprise.

If you do not want to install all features that are installed automatically or by default, you can use the `ADDLOCAL` MSI property to selectively install individual setup options and features. For details about the `ADDLOCAL` property, see Table 3-5. MSI Command-Line Options and MSI Properties.

You can modify features by using the `ADDLOCAL` and `REMOVE` MSI properties.

You can use the following PowerShell command to query the registry of installed components on the system where Horizon Agent is installed for the ModifyPath base command line:

```
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object
DisplayName, ModifyPath |
Where-Object {$_.DisplayName -eq 'VMware Horizon Agent'} | Format-Table –AutoSize
```

The output:

```
DisplayName               ModifyPath
VMware Horizon Agent      MsiExec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111}
```

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon 8 Installation and Upgrade* document.
- Prepare the guest operating system for desktop deployment. See Prepare a Guest Windows Operating System for Remote Desktop Deployment.
- To use Windows Server as a single-session remote desktop or as an RDSH host, perform the steps described in Prepare Windows Server Operating Systems for Desktop Use.

  Note The Horizon Agent installer does not automatically install any role in silent mode. If you want RDS mode, then pre-install the RDSH role on the system.

- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.

  The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

- Verify that you have administrative rights on the virtual machine or physical PC.
- Familiarize yourself with the Horizon Agent custom setup options. See Custom Setup Options for Horizon Agent for Windows .
- Familiarize yourself with the MSI installer command-line options. See Microsoft Windows Installer Command-Line Options.
- Familiarize yourself with the silent installation properties available with Horizon Agent. See Silent Installation Properties for Horizon Agent for Windows.
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *Horizon Overview and Deployment Planning* document for more information.
- Verify that the latest Windows Update patches are installed on the guest operating systems on which you plan to install Horizon Agent silently. In certain cases, an interactive installation by an administrator might be required to execute pending Windows Update patches. Verify that all OS operations and subsequent reboots are completed.

Install Horizon Agent Silently By Entering Parameters on the Command Line

1 Open a Windows command prompt on the virtual machine or physical PC.

The following example installs Horizon Agent with the components Core, VMware Blast, PCoIP, Unity Touch, PSG, USB redirection, and Real-Time Audio-Video components.

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v "/qn
VDM_VC_MANAGED_AGENT=1 ADDLOCAL=Core,USB,RTAV"
```

The following example installs Horizon Agent on an unmanaged computer and registers the desktop with the specified Connection Server, `cs1.companydomain.com`. In addition, the installer installs the Core, VMware Blast, PCoIP, Unity Touch, PSG, VMware Integrated Printing, and USB redirection components.

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v "/qn
VDM_VC_MANAGED_AGENT=0 VDM_SERVER_NAME=cs1.companydomain.com
VDM_SERVER_USERNAME=admin.companydomain.com VDM_SERVER_PASSWORD=secret
ADDLOCAL=Core,PrintRedir,USB"
```

The following example modifies and removes the USB component from an existing installation: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v "/qn REMOVE=USB"`

ProductCode-driven command line example: `msiexec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111} /qn REMOVE=USB`

The following example modifies the agent installation by replacing Horizon Performance Tracker with the Horizon Help Desk Tool: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v "/qn ADDLOCAL=HelpDesk REMOVE=PerfTracker”`

ProductCode-driven command line example: `msiexec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111} /qn ADDLOCAL=HelpDesk REMOVE=PerfTracker`

The following example modifies the agent installation by adding serial port and scanner redirection: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v "/qn ADDLOCAL=SerialPortRedirection,ScannerRedirection”`

ProductCode-driven command line example: `msiexec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111} /qn ADDLOCAL=SerialPortRedirection,ScannerRedirection`

Note If you install Horizon Agent on a Windows Server machine, and you intend to configure the machine as a single-user Horizon desktop rather than as an RDS host, you must include the `VDM_FORCE_DESKTOP_AGENT=1` property in the installation command. This requirement applies to machines that are managed by vCenter Server and unmanaged machines.

When the installation is complete, if the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See Configure a Virtual Machine with Multiple NICs for Horizon Agent.

Install Horizon Agent Silently Using a Settings File

1 Create a text file containing the parameters you want to use for the installation.

- The file can be located on either a local or network drive. Using mapped drives is also supported.
- The file can have any extension, but must be text-only.
- Each parameter must be on its own line.

- Any other text (besides the parameters themselves) must be commented out using a hash sign (#) at the beginning of the line.
- Both whitespace and empty newlines are allowed in the file.

Note If you install Horizon Agent on a Windows Server machine, and you intend to configure the machine as a single-user Horizon desktop rather than as an RDS host, you must include the `VDM_FORCE_DESKTOP_AGENT=1` property in the settings file. This requirement applies to machines that are managed by vCenter Server and unmanaged machines.

Attention The installer does not process passwords. If your file includes a known password property such as VDM_SERVER_PASSWORD, the installer fails to parse the file and returns an error. To include a password, you must enter it manually on the command line. When you enter a password in this way, it is passed only once and is not logged anywhere.

2 Open a Windows command prompt on the virtual machine or physical PC and enter the following.

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v SETTINGS_FILE=<file
path>
```

For example:

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v
SETTINGS_FILE=C:\Users\vmware\desktop\demo\agent-settings.txt
```

When the installation is complete, if the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See Configure a Virtual Machine with Multiple NICs for Horizon Agent.

Microsoft Windows Installer Command-Line Options

To install VMware Horizon 8 components silently, you must use Microsoft Windows Installer (MSI) command-line options and properties. The Horizon 8 component installers are MSI programs and use standard MSI features.

For details about MSI, see the Microsoft Web site. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library Web site and search for MSI command-line options. To see MSI command-line usage, you can open a command prompt on the Horizon 8 component computer and type `msiexec /?`.

To run a Horizon 8 component installer silently, you begin by silencing the bootstrap program that extracts the installer into a temporary directory and starts an interactive installation.

At the command line, you must enter command-line options that control the installer's bootstrap program.

Table 3-4. Command-Line Options for a Horizon 8 Component's Bootstrap Program

Option	Description
`/s`	Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs. For example: `VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s` The `/s` option is required to run a silent installation.
`/v" MSI_command_line_options"`	Instructs the installer to pass the double-quote-enclosed string that you enter at the command line as a set of options for MSI to interpret. You must enclose your command-line entries between double quotes. Place a double quote after the `/v` and at the end of the command line. For example: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"command_line_options"` To instruct the MSI installer to interpret a string that contains spaces, enclose the string in two sets of double quotes. For example, you might want to install the Horizon 8 component in an installation path name that contains spaces. For example: `VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""` In this example, the MSI installer passes on the installation-directory path and does not attempt to interpret the string as two command-line options. Note the final double quote that encloses the entire command line. The `/v"command_line_options"` option is required to run a silent installation.

You control the remainder of a silent installation by passing command-line options and MSI property values to the MSI installer, `msiexec.exe`. The MSI installer includes the Horizon 8 component's installation code. The installer uses the values and options that you enter in the command line to interpret installation choices and setup options that are specific to the Horizon 8 component.

Table 3-5. MSI Command-Line Options and MSI Properties

MSI Option or Property	Description
`/qn`	Instructs the MSI installer not to display the installer wizard pages. For example, you might want to install Horizon Agent silently and use only default setup options and features: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn"` Alternatively, you can use the `/qb` option to display a basic progress dialog box in a noninteractive, automated installation. The `/qn` or `/qb` option is required to run a silent installation. For information about additional `/q` parameters, see the Microsoft Dev Center website.
`INSTALLDIR`	Specifies an alternative installation path for the Horizon 8 component. Use the format `INSTALLDIR=path` to specify an installation path. You can ignore this MSI property if you want to install the Horizon 8 component in the default path. This MSI property is optional.

Table 3-5. MSI Command-Line Options and MSI Properties (continued)

MSI Option or Property	Description
`ADDLOCAL`	Determines the component-specific options to install. In an interactive installation, the Horizon 8 installer displays custom setup options that you can select or deselect. In a silent installation, you can use the `ADDLOCAL` property to selectively install individual setup options by specifying the options on the command line. Options that you do not explicitly specify are not installed. In both interactive and silent installations, the Horizon 8 installer automatically installs certain features. You cannot use `ADDLOCAL` to control whether or not to install these non-optional features. Type `ADDLOCAL=ALL` to install all custom setup options that can be installed during an interactive installation, including those that are installed by default and those that you must select to install, except NGVC. NGVC and SVIAgent are mutually exclusive. The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and all features that are supported on the guest operating system: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"` If you do not use the `ADDLOCAL` property, the custom setup options that are installed by default and the automatically installed features are installed. Custom setup options that are off (unselected) by default are not installed. The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and the on-by-default custom setup options that are supported on the guest operating system: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn"` To specify individual setup options, type a comma-separated list of setup option names. Do not use spaces between names. Use the format `ADDLOCAL=`*`value,value,value...`*. You must include `Core` when you use the `ADDLOCAL=`*`value,value,value...`* property. The following example installs Horizon Agent with the Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and Instant Clone Agent features: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC` The preceding example does not install other components, even those that are installed by default interactively. The `ADDLOCAL` MSI property is optional.
`REBOOT`	You can use the `REBOOT=ReallySuppress` option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.
`REINSTALL`	You can use the `REINSTALL=ALL` option to install a Horizon Agent patch. The following example installs the patch: `msiexec /p VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.msp /qn REINSTALL=ALL` This MSI property is optional.

Table 3-5. MSI Command-Line Options and MSI Properties (continued)

MSI Option or Property	Description
`REMOVE`	You can use the `REMOVE=<value>` option to remove a feature. The following example uninstalls the USB feature: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"` This MSI property is optional.
`/l*v` *`log_file`*	Writes logging information into the specified log file with verbose output. For example: `/l*v ""%TEMP%\vmmsi.log""` This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The `/l*v` option is optional.

Silent Installation Properties for Horizon Agent for Windows

You can include specific properties when you silently install Horizon Agent for Windows from the command line. You must use a *`PROPERTY=value`* format so that Microsoft Windows Installer (MSI) can interpret the properties and values. A silent upgrade uses the same install commands. You can also modify already installed Horizon Agent components silently.

The following table shows the Horizon Agent silent installation properties that you can use at the command-line.

Table 3-6. MSI Properties for Silently Installing Horizon Agent

MSI Property	Description	Default Value
`ENABLE_UNC_REDIRECTION`	Specifies whether the UNC Path Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which UNCs to redirect. See "Configuring UNC Path Redirection" in the *Horizon Remote Desktop Features and GPOs* document. This MSI property is optional.	0
`HORIZON_MONITOR_ENABLED`	Specifies whether to enable or disable Horizon monitoring mode. This flag works only if you have VMware Horizon Cloud Service - next-gen installed in your environment. A value of 1 enables Horizon monitoring mode. A value of 0 disables Horizon monitoring.	0
`IGNORE_DOTNET_CHECK`	Determines whether the installer checks for a minimum .NET version. By default, when Horizon Performance Tracker is selected, the installer performs a pre-check to confirm that .NET 4.6.2 or later is installed, and stops the install process if it is not. A value of 1 cancels this pre-check. A value of 0 allows the pre-check to proceed.	`%ProgramFiles%\VMware\VMware View\Agent`

Table 3-6. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
`INSTALLDIR`	Path and folder in which the Horizon Agent software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	
`RDP_CHOICE`	Determines whether to enable Remote Desktop Protocol (RDP) on the desktop. A value of 1 enables RDP. A value of 0 leaves the RDP setting deactivated. This MSI property is optional.	1
`SUPPRESS_RUNONCE_CHECK`	Ignores pending Windows Update tasks scheduled at the next operating system reboot in the `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` and `RunOnceEx` keys. Using this flag allows concurrent installation but does not guarantee the installation outcome when the system updates affect the Horizon Agent run-time dependencies. This MSI property is optional.	None
`URL_FILTERING_ENABLED`	Specifies whether the URL Content Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which URLs to redirect. See "Configuring URL Content Redirection" in the *Horizon Remote Desktop Features and GPOs* document. This MSI property is optional.	0
`VDM_SKIP_BROKER_REGISTRATION`	A value of 1 skips unmanaged desktops.	None
`VDM_VC_MANAGED_AGENT`	Determines whether vCenter Server manages the virtual machine on which Horizon Agent is installed. A value of 1 configures the desktop as a vCenter Server-managed virtual machine. A value of 0 configures the desktop as unmanaged by vCenter Server. This MSI property is required. **Note** The installer repair option is not supported for an unmanaged installation. Repairing such an installation results in an installation of a managed Horizon Agent.	None
`VDM_REINSTALL`	Specifies a list of already installed features delimited by commas that are to be reinstalled, applicable only in silent mode.	None
`VDM_REINSTALLMODE`	A string containing letters that specifies the type of reinstall to perform, applicable only in silent mode. See https://learn.microsoft.com/en-us/windows/win32/msi/reinstallmode for details on which options to use.	None

Table 3-6. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
`VDM_SERVER_NAME`	Host name or IP address of the Connection Server instance on which the Horizon Agent installer registers an unmanaged desktop. This property applies to unmanaged desktops only. For example: `VDM_SERVER_NAME=10.123.01.01` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
`VDM_SERVER_USERNAME`	User name of the administrator on the Connection Server instance. This MSI property applies only to unmanaged desktops. For example: `VDM_SERVER_USERNAME=domain\username` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops managed by vCenter Server.	None
`VDM_SERVER_PASSWORD`	Connection Server administrator user password. For example: `VDM_SERVER_PASSWORD=secret` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
`VDM_IP_PROTOCOL_USAGE`	Specifies the IP version that Horizon Agent uses. Valid values are IPv4 and IPv6.	IPv4
`VDM_FIPS_ENABLED`	Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will stop.	0
`VDM_FORCE_DESKTOP_AGENT`	If you install Horizon Agent on a Windows Server machine and configure it as a single-user Horizon desktop rather than as an RDS host, set the value to 1. This requirement applies to machines managed by vCenter Server and unmanaged machines. For non-server Windows guests that host application sessions, set the value to 0. This MSI property is optional.	0

In a silent installation command, you can use the `ADDLOCAL` property to specify options that the Horizon Agent installer configures.

The following table shows the Horizon Agent options that you can enter at the command line. These options have corresponding setup options that you can deselect or select during an interactive installation.

When you do not use the `ADDLOCAL` property at the command line, Horizon Agent installs all of the options that are installed by default during an interactive installation, if they are supported on the guest operating system. When you use `ADDLOCAL=ALL`, Horizon Agent installs all of the following options, both on-by-default and off-by-default, if they are supported on the guest operating system.

For more information, see the `ADDLOCAL` table entry in Microsoft Windows Installer Command-Line Options.

If you use `ADDLOCAL` to specify features individually (you do not specify `ADDLOCAL=ALL`), you must always specify `Core`.

You can modify features by using the `ADDLOCAL` and `REMOVE` MSI properties. Use the following PowerShell command to query the registry of installed components on the system where Horizon Agent is installed for the ModifyPath base command line:

```
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* |
        Select-Object DisplayName, ModifyPath | Where-Object {$_.DisplayName -eq 'VMware
Horizon
        Agent'} | Format-Table –AutoSize
```

The output:

```
DisplayName               ModifyPath
          VMware Horizon Agent      MsiExec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111}
```

The following example modifies and removes the USB component from an existing installation: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"`

The following example modifies the agent installation by replacing Horizon Performance Tracker with the Horizon Help Desk Tool: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=HelpDesk REMOVE=PerfTracker”`

The following example modifies the agent installation by adding serial port and scanner redirection: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=SerialPortRedirection,ScannerRedirection”`

Table 3-7. Horizon Agent Silent Installation Options and Interactive Custom Setup Options

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When ADDLOCAL Is Not Used
Core	The core Horizon Agent functions. If you specify `ADDLOCAL=ALL`, the Core features are installed.	Yes
PCoIP	PCoIP Protocol Agent	Yes
USB	USB Redirection	No
NGVC	Instant Clone Agent	No
RTAV	Real-Time Audio-Video	Yes

Table 3-7. Horizon Agent Silent Installation Options and Interactive Custom Setup Options (continued)

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When `ADDLOCAL` Is Not Used
ClientDriveRedirection	Client Drive Redirection	Yes
SerialPortRedirection	Serial Port Redirection	No
ScannerRedirection	Scanner Redirection	No
GEOREDIR	Geolocation Redirection	No
V4V	Horizon Monitoring Service Agent	Yes
SmartCard	Smartcard This feature is not installed by default in an interactive installation.	No
VmwVaudio	VMware Audio (virtual audio driver)	Yes
VmwVidd	VMware Indirect Display Driver	Yes **Note** VmwVidd is installed and marked as Local in the registry only if: - Desktop Mode Windows Server is RS4 and above (OS build 17134 - version 1803), `or` - Server is 19H1 and above (OS build 18362 - version 1903) VmwVidd is installed and set as `Absent` in the registry in Windows Server 2019 (version 1809) std and datacenter with the RDS role. VmwVidd will be installed and set as `Local` in the registry in Windows Server 2022 with the RDS role.
TSMMR	Windows Media Multimedia Redirection (MMR)	Yes
RDP	Enables RDP in the registry if you use the `RDP_CHOICE=1` property on the command line or select RDP as the default display protocol when you create or edit a desktop pool. This feature is hidden during interactive installations.	Yes
RDSH3D	3D rendering on RDS hosts	No
BlastUDP	UDP Transport support for Blast	Yes
SdoSensor	SDO Sensor Redirection	No
PerfTracker	Horizon Performance Tracker	No

Table 3-7. Horizon Agent Silent Installation Options and Interactive Custom Setup Options (continued)

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When ADDLOCAL Is Not Used
HelpDesk	Horizon Help Desk Tool	Yes
PrintRedir	VMware Integrated Printing	Yes
PSG	This feature sets a registry entry that tells Connection Server whether Horizon Agent is using IPv4 or IPv6.	Yes

Install or Uninstall a Horizon Agent for Windows Patch Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install and uninstall a Horizon Agent patch. In a silent installation, you use the command line and do not have to respond to wizard prompts.

Prerequisites

- Verify that you have administrative rights on the virtual machine or physical PC.
- Select the product version and download the Horizon Agent Update Patch installer file from the VMware product page at https://customerconnect.vmware.com/downloads/info/slug/desktop_end_user_computing/vmware_horizon/2303.

  The installer filename is `VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

Procedure

1 Open a Windows command prompt as administrator on the virtual machine or physical PC.

2 To install a Horizon Agent patch where Horizon Agent is installed, run the .exe file: `msiexec /p VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.exe /qn REINSTALL=ALL”`

  After installing the patch, verify the patch build number is updated in the registry: `HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent` and `HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber`.

3 To uninstall a Horizon Agent patch where Horizon Agent is installed, run a PowerShell script: `remove-patch.ps1`

  ProductCode-driven command line example: `msiexec /package {product_code} /uninstall {patch_guid} /passive`

  After uninstalling the patch, check the registry: `HKLM:\SOFTWARE\WOW6432Node\VMware, Inc.\AgentVersions!view-agent` and `HKLM:\SOFTWARE\VMware, Inc.\Vmware VDM!BuildNumber` that no reference of the patch exists. Verify the services are in the same state as they were before uninstalling the patch.

Preparing a Windows Golden Image Virtual Machine for Instant Clones

To deploy a Windows instant-clone desktop pool, you must first prepare a golden image virtual machine in vCenter Server.

- Configure a Windows Golden Image Virtual Machine

  After creating a virtual machine that you plan to use as a golden image, configure the Windows environment.

- Activating Windows on Instant Clones

  To make sure that Windows is properly activated when the clones are created, you must use Microsoft volume activation on the golden image virtual machine before creating an instant-clone desktop. The volume-activation technology requires a volume license key.

- Deactivate Windows Hibernation in the Golden Image

  The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Deactivating hibernation reduces the size of an instant clone's virtual disk.

- Choosing ClonePrep or Sysprep for Customizing Your Windows Virtual Desktops

  There are two options for customizing instant-clone Windows virtual machines: VMware ClonePrep or Microsoft Sysprep.

- Creating Customization Specifications When Using Sysprep for Desktop Customization

  When you customize a clone using Sysprep, you need to provide a customization specification.

- Increase the Timeout Limit for ClonePrep Customization Scripts on a Windows Machine

  ClonePrep post-synchronization or power-off scripts have a timeout limit of 20 seconds. You can increase this limit by changing the `ExecScriptTimeout` Windows registry value on the golden image virtual machine.

- Compute Profiles and Windows Golden Images

  The VMware Horizon 8 compute profile feature significantly improves golden image management and reduces the number of golden images required to create desktop pools for different requirements.

Configure a Windows Golden Image Virtual Machine

After creating a virtual machine that you plan to use as a golden image, configure the Windows environment.

Prerequisites

- Verify that you prepared a virtual machine to use for deploying remote desktops. See Creating a Windows Virtual Machine for Cloning.

The golden image can either belong to the same Active Directory domain as the domain that the desktop machines will join or be a member of a workgroup.

- Verify that the virtual machine was not converted from an instant clone.

  Important You also cannot use an instant clone as a golden image.

- When you install Horizon Agent on the golden image, verify that the **VMware Horizon Instant Clone Agent** option for instant clones is selected. See Install Horizon Agent on a Virtual Machine.
- To deploy Windows machines, configure a volume license key and activate the golden image virtual machine's operating system with volume activation. See Activating Windows on Instant Clones.
- Verify that you followed the best practices for optimizing the operating system. See Optimize Guest Windows Operating System Performance.
- Familiarize yourself with the procedure for disabling searching Windows Update for device drivers. See the Microsoft Technet article, "Disable Searching Windows Update for Device Drivers" at http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx.

Procedure

- Verify that the system disk contains a single volume.
- Verify that the virtual machine does not contain an independent disk. However, the golden image virtual machine can contain multiple disks.

  An independent disk is excluded when you take a snapshot of the virtual machine. Clones are based on a snapshot and therefore will not contain the independent disk.

- Deactivate the hibernation option to reduce the size of each clone's virtual disk.
- Before you take a snapshot of the golden image, disable searching Windows Update for device drivers.

  This Windows feature can interfere with the customization process. As each clone is customized, Windows might search for the best drivers on the Internet for that clone, resulting in delays.

- In vSphere Client, disable the vApp Options setting on the golden image virtual machine.
- Disable the HotPlug capability on removable devices. See KB 1012225.

What to do next

Use vSphere Client to take a snapshot of the golden image virtual machine in its powered-down state. This snapshot is provides the base image for the clones.

Important Before you take a snapshot, shut down the golden image virtual machine.

Activating Windows on Instant Clones

To make sure that Windows is properly activated when the clones are created, you must use Microsoft volume activation on the golden image virtual machine before creating an instant-clone desktop. The volume-activation technology requires a volume license key.

Two volume-activation models are supported for instant clones:

- Key Management Service (KMS) allows organizations to activate systems within their own network. Microsoft recommends using this method for large scale deployments.
- Multiple Activation Key (MAK) activates systems on a one-time basis, using Microsoft's hosted activation services.

MAK treats each activated clone as a computer with a newly issued license. When an instant clone is refreshed on log off or an instant clone push image operation is performed, an additional MAK activation may be consumed based on Microsoft's proprietary logic. Each MAK license has a pre-determined number of allowed activations based on your Volume Licensing Agreement. Therefore, depending on your operations, you will need to request an increase in MAK activation quantity per Microsoft guidance. Hence, KMS activation is the preferred approach.

Reach out to your Microsoft dealer to acquire the appropriate volume license key and configure volume activation. For the latest information from Microsoft regarding KMS and MAK, see https://learn.microsoft.com/en-us/licensing/products-keys-faq.

Note Active Directory-based activation is not supported for any of the above volume-activation models.

Activating Windows with Key Management Service (KMS)

You must activate Windows on the golden image before creating an instant-clone desktop. Follow the steps below to activate Windows with KMS.

Note If you set up a new KMS server and use ClonePrep to create instant-clone desktop pools, the KMS client count might not increment and the instant-clone might not be able to activate Windows. For more information, see the VMware Knowledge Base (KB) article http://kb.vmware.com/kb/2048742.

1. Acquire a KMS license key.
2. Invoke a script to remove the existing license. For more information, see the Microsoft Windows documentation to remove the Windows license key using a command.
3. Restart Windows.
4. Invoke a script that uses KMS licensing to activate Windows.

KMS treats each activated clone as a computer with a newly issued license.

Activating Windows with Multiple Activation Key (MAK)

You must activate Windows on the golden image before creating an instant-clone desktop. Follow the steps below to activate Windows with MAK.

1. Acquire a MAK license key.
2. Invoke a script to remove the existing license. For more information, see the Microsoft Windows documentation to remove the Windows license key using a command line option.
3. Restart Windows.
4. Run the following command to configure MAK:

   `slmgr /ipk` *MAK_License_Key*

Deactivate Windows Hibernation in the Golden Image

The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Deactivating hibernation reduces the size of an instant clone's virtual disk.

Caution When you make hibernation unavailable, hybrid sleep does not work. Users can lose data if a power loss occurs.

Procedure

1. In vSphere Client, select the golden image virtual machine and select **Open Console**.
2. Log in as an administrator.
3. Deactivate the hibernation option.
   1. Click **Start** and type **`cmd`** in the **Start Search** box.
   2. In the search results list, right-click **Command Prompt** and click **Run as Administrator**.
   3. At the **User Account Control** prompt, click **Continue**.
   4. At the command prompt, type **`powercfg.exe /hibernate off`** and press Enter.
   5. Type **`exit`** and press Enter.

Choosing ClonePrep or Sysprep for Customizing Your Windows Virtual Desktops

There are two options for customizing instant-clone Windows virtual machines: VMware ClonePrep or Microsoft Sysprep.

ClonePrep is a VMware customization process run during instant clone deployment to personalize each desktop clone created from the parent image. During the initial startup of each desktop, ClonePrep:

- Creates a new computer account in Active Directory for each desktop.
- Gives the instant clone desktop a new name.
- Joins the desktop to the appropriate domain.

Sysprep is a Microsoft tool to deploy the configured operation system installation from a base image. The desktop can then be customized based on an answer script. Sysprep can modify a larger number of configurable parameters than ClonePrep, but ClonePrep is significantly faster. Majority of instant clone customers choose ClonePrep

It is recommended that you use ClonePrep unless there are specific Sysprep capabilities required for your environment. For information on the differneces between these methods, see Knowledge Base article 2003797.

Creating Customization Specifications When Using Sysprep for Desktop Customization

When you customize a clone using Sysprep, you need to provide a customization specification.

You create customization specifications by using the Customization Specification wizard in vSphere. See the *vSphere Virtual Machine Administration* document for information on using the Customization Specification wizard.

It is recommended that you test a customization specification in vSphere before you use it to create a desktop pool.

Note the following requirements and limitations:

- Windows is the only supported operating system for Instant Clone desktops with Sysprep customization.
- Linux is not supported as the target guest operating system.
- When you use a Sysprep customization specification to join a Windows desktop to a domain, you must use the fully qualified domain name (FQDN) of the Active Directory domain. You cannot use the NetBIOS name.
- Using a custom Sysprep answer file is not supported.
- On the **Computer Name** page of the wizard, the **Use the virtual machine name** option must be selected.
- The **Automatically logon as Administrator** option is not supported. If you select this option during the customization process, the system ignores the setting.
- Only single NIC configurations are supported.
- Entering FQDN and AD domain credentials different from those configured for the pool is not supported. If you enter these values, the system ignores them and joins the domain configured for the pool.
- If any explicit DNS server setup is required for the domain join, you must select **Manually Select custom settings** on the **Network** page and enter the settings.

Increase the Timeout Limit for ClonePrep Customization Scripts on a Windows Machine

ClonePrep post-synchronization or power-off scripts have a timeout limit of 20 seconds. You can increase this limit by changing the `ExecScriptTimeout` Windows registry value on the golden image virtual machine.

Instead of increasing the timeout limit you can also use your customization script to launch another script or process that performs the long-running task.

Note Some ClonePrep customization scripts can finish running within the 20-second limit. Test your scripts before you increase the limit.

Procedure

1 On the golden image virtual machine, start the Windows Registry Editor.

   a Select **Start > Command Prompt**.

   b At the command prompt, type **regedit**.

2 In the Windows registry, locate the `vmware-viewcomposer-ga` registry key.

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga`

3 Click **Edit** and modify the registry value.

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

   The default value is 20000 milliseconds.

Compute Profiles and Windows Golden Images

The VMware Horizon 8 compute profile feature significantly improves golden image management and reduces the number of golden images required to create desktop pools for different requirements.

Please refer to Instant Clone Desktop Pools to learn more about this feature.

Using the VMware Indirect Display Driver on Windows Desktops

The VMware Indirect Display Driver is a hypervisor-agnostic display driver that supports a variety of system environments, from on-premises ESXi-hosted virtual machines (VMs) to cloud-based VMs. It is distributed as part of Horizon Agent for Windows and works with both hardware GPUs and software rasterizers.

Prerequisites

Before you can use the VMware Indirect Display Driver, you must do the following.

- Verify that the agent machine is running Windows 10, version 1803 or later.

- Install Horizon Agent on the machine, as described in Install Horizon Agent on a Windows Virtual Machine. By default, the VMware Indirect Display Driver is automatically installed as part of the agent software.

  If you are specifying feature options with a silent installation, include the `VmwVidd` option as described in Silent Installation Properties for Horizon Agent for Windows.

Capabilities of the VMware Indirect Display Driver

By leveraging the rendering and encoding capabilities of the VM's underlying hardware GPU, the VMware Indirect Display Driver allows applications to be rendered optimally at high frame rates. This functionality offers performance advantages when working with multi-session pools and high-workload 3D applications such as design and modeling software.

The VMware Indirect Display Driver also supports software rasterizers such as the Microsoft Windows Advance Rasterization Platform (WARP).

The VMware Horizon Indirect Display Driver is optimized to perform well with VMware Blast Extreme, resulting in lower memory consumption and in certain cases, lower CPU and GPU utilization.

Configuring the Display Driver Priority

By default, the VMware Indirect Display Driver serves as the fallback display driver for remote sessions, provided that sufficient system resources are available. The Horizon display protocol chooses a display driver according to the following priority:

1. The protocol first attempts to set up the session's display topology using the active GPU or hypervisor display driver.
2. If the hypervisor or GPU display driver does not support the requested display topology or is not functioning, the protocol uses the VMware Indirect Display Driver.

In an environment such as Horizon Cloud on Azure where neither the hypervisor not the GPU display driver are available, the VMware Indirect Display Driver serves as the primary display driver.

You can change the default priority rules to make the VMware Indirect Display Driver the primary display driver used first for remote sessions. In `HKLM\Software\Policies\VMware, Inc.\VMware Blast\Config`, configure the following registry setting:

```
PixelProviderForceViddCapture REG_SZ : 1
```

Accessing the Hypervisor Remote Console

The VMware Indirect Display Driver has no direct communication with the hypervisor and does not support the use of hypervisor remote consoles such as the VMware Remote Console Application.

If you need access to a hypervisor remote console, you can install the hypervisor display driver and deactivate the VMware Indirect Display Driver.

Alternatively, you can configure a registry setting to temporarily turn off the VMware Indirect Display Driver after a remote session ends and restore access to the hypervisor remote console. This configuration allows the VMware Indirect Display Driver to be used only during remote sessions and allows access to the hypervisor remote console otherwise. You might see a rearrangement of application windows as control of the display topology passes to the hypervisor display driver.

In `HKLM\Software\Policies\VMware, Inc.\VMware Blast\Config`, configure the following registry setting:

```
HypervisorConsoleForcedEnabled REG_SZ : 1
```

Activating Low Latency Mode

You can use the VMware Indirect Display Driver in low latency mode, which allows applications to render at a higher frame rate to reduce latency from user input. Since the higher frame rate results in increased consumption of CPU and GPU resources, low latency mode is deactivated by default.

For best results with low latency mode, ensure that the agent machine is using a hardware-accelerated GPU. Actual user experience may vary based on factors such as network conditions and client hardware capability.

To activate low latency mode, configure the following registry setting in `HKLM\Software\Policies\VMware, Inc.\VMware Blast\Config`:

```
PixelProviderLowLatencyEnabled REG_SZ : 1
```

Feature Limitations of the VMware Indirect Display Driver

The VMware Indirect Display Driver has the following feature issues and limitations.

- A ghost monitor appears in the Windows system display settings. For more information, see VMware Knowledge Base (KB) article 88560.
- Users might experience issues when using the cursor in Microsoft Excel. For more information, see KB article 93017.

Creating and Preparing a Linux Virtual Machine for Cloning

To create and prepare a VMware vSphere-based Linux virtual machine (VM) for use in an automated desktop pool, follow the documentation links on this page.

Overview of Configuration Steps for Setting Up Linux Desktops

When you configure Linux desktops in a VMware Horizon 8 environment, you must follow a different sequence of steps depending on whether you install 2D graphics or 3D graphics on the virtual machines.

2D Graphics - Overview of Configuration Steps

For 2D graphics, take the following steps:

1 Review the system requirements for setting up a Linux desktop deployment. See System Requirements for Horizon Agent for Linux.

2 Create a virtual machine in vSphere and install the Linux operating system. See Create a Virtual Machine and Install Linux.

3 Prepare the guest operating system for deployment as a desktop in a Horizon 8 environment. See Prepare a Linux Machine for Remote Desktop Deployment.

4 Configure the Linux guest operating system to authenticate with Active Directory. This step is implemented with 3rd-party software, based on the requirements in your environment. See Integrating Linux Desktops with Active Directory for more information.

5 Install Horizon Agent on the Linux virtual machine. See Install Horizon Agent on a Linux Machine.

6 Create a desktop pool based on the configured Linux virtual machine.

3D Graphics - Overview of Configuration Steps

You must complete the NVIDIA GRID vGPU configuration on the Linux virtual machines before you install Horizon Agent on the machines and deploy a desktop pool using Horizon Console.

1 Review the system requirements for setting up a Linux desktop deployment in a Horizon 8 environment. See System Requirements for Horizon Agent for Linux.

2 Create a virtual machine in vSphere and install the Linux operating system. See Create a Virtual Machine and Install Linux.

3 Prepare the guest operating system for deployment as a desktop in a Horizon 8 environment. See Prepare a Linux Machine for Remote Desktop Deployment.

4 Configure the Linux guest operating system to authenticate with Active Directory. This step is implemented with 3rd-party software, based on the requirements in your environment. See Integrating Linux Desktops with Active Directory for more information.

5 Configure 3D capabilities on your ESXi hosts and the Linux virtual machine. For more information, see Chapter 5 Setting Up Graphics for Linux Virtual Machines.

6 Install Horizon Agent on the Linux virtual machine. See Install Horizon Agent on a Linux Machine.

7 Create a desktop pool based on the configured Linux virtual machine.

System Requirements for Horizon Agent for Linux

To install Horizon Agent for Linux, you must meet certain requirements for the Linux operating system, Linux virtual machine, VMware Horizon 8 system components, and VMware vSphere platform.

Supported Linux Distributions for Horizon Agent

The following table lists the Linux operating systems that have been tested and are supported for Horizon Agent.

Table 3-8. Supported Linux Operating Systems for Horizon Agent

Linux Distribution	Architecture
Ubuntu 20.04 and 22.04	x64
Debian 10.13, 11.7, and 12.2	x64
Red Hat Enterprise Linux (RHEL) Workstation 7.9, 8.6, 8.8, 8.9, 9.0, 9.1, 9.2, and 9.3	x64
Red Hat Enterprise Linux (RHEL) Server 7.9, 8.6, 8.8, 8.9, 9.0, 9.1, 9.2, and 9.3	x64
Rocky Linux 8.9 and 9.3	x64
CentOS 7.9	x64
SUSE Linux Enterprise Desktop (SLED) 15 SP4 and 15 SP5	x64
SUSE Linux Enterprise Server (SLES) 15 SP4 and 15 SP5	x64

Note Horizon Agent has dependency packages on some Linux distributions. See Install Linux Dependency Packages for Horizon Agent for more information.

Some features are supported on a limited subset of Linux operating systems. For more information, see the section of this document that discusses the specific feature.

The `install_viewagent.sh` installation script provides a `--force` parameter that forces the installation of Horizon Agent on Linux distributions not listed in the test support matrix. See Command-line Options for Installing Horizon Agent for Linux .

Required Platform and Software Versions

To install and use Horizon Agent for Linux, your deployment must meet certain requirements for the vSphere platform, Horizon Connection Server, and Horizon Client software.

Table 3-9. Required Platform VMware Horizon Software Versions

Platform and Software	Supported Versions
vSphere platform version	■ vSphere 8.0 or later release ■ vSphere 7.0 or later release
VMware Horizon 8 environment	■ Horizon Connection Server 2312
Horizon Client software	■ Horizon Client for Android 2312 ■ Horizon Client for Windows 2312 ■ Horizon Client for Linux 2312 ■ Horizon Client for Mac 2312 ■ Horizon Client for iOS 2312 ■ HTML Access 2312 on Chrome and Firefox ■ Zero clients that support the VMware Blast protocol **Note** Teradici PCoIP zero clients are not supported.

Ports Used by Linux Desktops

To enable connection sessions, Linux desktops must support incoming TCP connections from Horizon Client devices, Unified Access Gateway, and Horizon Connection Server.

On Ubuntu and Debian distributions, the `iptables` firewall is configured by default with an input policy of ACCEPT.

On RHEL, Rocky Linux, and CentOS distributions, where possible, the Horizon Agent installer script configures the `iptables` firewall with an input policy of ACCEPT. To ensure support of incoming connections, verify that `iptables` has an input policy of ACCEPT for new connections through the Blast port, 22443.

When you enable Blast Secure Gateway (BSG), client connections are directed from a Horizon Client device through the BSG on the Horizon Connection Server to the Linux desktop. When you do not enable BSG, connections are made directly from the Horizon Client device to the Linux desktop.

For detailed information on the ports used by Horizon Agent on Linux desktops, see the *Horizon Security* document and the Network Ports in VMware Horizon guide.

Verify the Linux Account Used by Linux Virtual Machines

The following table lists the account name and account type used by Linux virtual machines.

Table 3-10. Account Name and Account Type

Account Name	Account Type	Used By
root	Linux OS built-in	Java Standalone Agent, `mksvchanserver`, shell scripts
vmwblast	Created by Linux Agent installer	VMwareBlastServer
<current login user>	Linux OS built-in or AD user or LDAP user	Python script

Desktop Environment

Horizon Agent for Linux supports multiple desktop environments on different Linux distributions. The following table lists the default desktop environments for each Linux distribution and the other desktop environments supported by Horizon Agent for Linux.

Table 3-11. Supported Desktop Environments

Linux Distribution	Default Desktop Environment	Desktop Environments Supported by Horizon Agent for Linux
Ubuntu	Gnome	Gnome Ubuntu, K Desktop Environment (KDE), MATE
Debian	Gnome	Gnome, KDE, MATE
RHEL and Rocky Linux 8.x/9.x	Gnome	Gnome
RHEL 7.9	Gnome	Gnome, KDE, MATE
CentOS 7.9	Gnome	Gnome, KDE
SLED/SLES	Gnome	Gnome

Note When using RHEL/CentOS 7.x and Ubuntu distributions, SSO fails to unlock a locked KDE session. You must manually enter your password to unlock the locked session.

To change the default desktop environment used on one of the supported Linux distributions, you must use the following steps and commands appropriate for your Linux desktop.

1 Install the supported Linux distribution's operating system with the default desktop environment setting.

2 Run the appropriate commands described in the following table for your specific Linux distribution.

Table 3-12. Commands to Install Desktop Environments

Linux Distribution	New Default Desktop Environment	Commands to Change the Default Desktop Environment
RHEL/CentOS 7.9	KDE	`yum groupinstall "KDE Plasma Workspaces"`

RHEL 7.9	MATE	`rpm -ivh https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-14.noarch.rpm`
		`yum groupinstall -y "MATE Desktop"`

Ubuntu	KDE	`apt install plasma-desktop`
Ubuntu	MATE	`apt install ubuntu-mate-desktop`

3 To begin using the new default desktop environment, restart the desktop.

If you enabled SSO on a Linux desktop that has multiple desktop environments installed, use the following information to select the desktop environment to use in an SSO session.

- For Ubuntu and RHEL/CentOS 7.x, use the information in the following table to set the `SSODesktopType` option in the `/etc/vmware/viewagent-custom.conf` file to specify the desktop environment to use with SSO.

  Table 3-13. SSODesktopType Option

Desktop Type	SSODesktopType Option Setting
MATE	SSODesktopType=UseMATE
GnomeUbuntu	SSODesktopType=UseGnomeUbuntu
GnomeFlashback	SSODesktopType=UseGnomeFlashback
KDE	SSODesktopType=UseKdePlasma
GnomeClassic	SSODesktopType=UseGnomeClassic

- For RHEL and Rocky Linux 9.x/8.x, for the SSO login session to use Gnome Classic, remove all the desktop startup files, except for the Gnome Classic startup file, from the `/usr/share/xsession` directory. For example, run the following set of commands as the root user:

  ```
  cd /usr/share/xsessions
  mkdir backup
  mv *.desktop backup
  mv backup/gnome-classic.desktop ./
  ```

After the initial setup, the end user must log out or reboot their Linux desktop to use Gnome Classic as the default desktop in their next SSO session.

If you deactivated SSO on a Linux desktop that has multiple desktop environments installed, you do not need to perform any of the previously described steps. The end users have to select their desired desktop environment when they log in to that Linux desktop.

Network Requirements

VMware Blast Extreme supports both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Network conditions affect the performances of UDP and TCP. To receive the best user experience, select UDP or TCP based on the network condition.

- Select TCP if the network condition is good, such as in a local area network (LAN) environment.
- Select UDP if the network condition is poor, such as in a wide area network (WAN) environment with packet loss and time delay.

Use a network analyzer tool, such as Wireshark, to determine whether VMware Blast Extreme is using TCP or UDP. Use the following set of steps, which use Wireshark, as a reference example.

1 Download and install Wireshark on your Linux VM.

   For RHEL/CentOS and Rocky Linux:

   ```
   sudo yum install wireshark
   ```

   For Ubuntu:

   ```
   sudo apt install tshark
   ```

2 Connect to the Linux desktop using VMware Horizon Client.

3 Open a terminal window and run the following command, which displays the TCP package or UDP package used by VMware Blast Extreme.

   ```
   sudo tshark -i any | grep 22443
   ```

USB Redirection and Client Drive Redirection (CDR) features are sensitive to network conditions. If the network condition is bad, such as a limited bandwidth with time delay and packet loss, the user experience becomes poor. In such condition, the end user might experience one of the following.

- Copying remote files can be slow. In this situation, transmit smaller sized files instead.
- USB device does not appear in the remote Linux desktop.
- USB data does not transfer completely. For example, if you copy a large file, you might get a file smaller in size than the original file.

VHCI Driver for USB Redirection

Note To determine the correct installation sequence for the VHCI driver, use the following guidelines:

- If you intend to install Horizon Agent using the `.tar.gz` tarball installer, you must first download and unpack the tarball installer, then install the VHCI driver, and then install Horizon Agent with the installation parameter for the USB redirection feature.
- If you intend to install Horizon Agent using the `.rpm` RPM installer, you must first install Horizon Agent, then install the VHCI driver, and then add the USB redirection feature to the Horizon Agent configuration.

For more information, see Install Horizon Agent on a Linux Machine.

The USB redirection feature has a dependency on the USB Virtual Host Controller Interface (VHCI) kernel driver. To support USB 3.0 and the USB redirection feature, you must install the VHCI driver by performing the following steps:

1. Download the USB VHCI source code from https://sourceforge.net/projects/usb-vhci/files/linux%20kernel%20module/.
2. Identify the full path to the VHCI patch file, depending on the Horizon Agent installer format. For guidelines, see the following examples.
   - (Tarball installer) If you download and unpack the tarball installer `VMware-horizonagent-linux-x86_64-`*`YYMM-y.y.y-xxxxxxx`*`.tar.gz` under the `/install_tmp/` directory, the *`full-path_to_patch-file`* is `/install_tmp/VMware-horizonagent-linux-x86_64-`*`YYMM-y.y.y-xxxxxxx`*`/resources/vhci/patch/vhci.patch`.
   - (RPM installer) If you download the RPM installer `VMware-horizonagent-linux-`*`YYMM-y.y.y-xxxxxxx`*`.el8.x86_64.rpm` and use it to install Horizon Agent, the *`full-path_to_patch-file`* is `/usr/lib/vmware/viewagent/resources/vhci/patch/vhci.patch`.
3. To compile the VHCI driver source code and install the resulting binary on your Linux system, use the commands listed in the following table. Replace *`full-path_to_patch-file`* in the commands with the file path that you identified in the previous step.

   For example, if the file path is `/install_tmp/VMware-horizonagent-linux-x86_64-`*`YYMM-y.y.y-xxxxxxx`*`/resources/vhci/patch/vhci.patch`, the `patch` command becomes:

   ```
   patch -p1 < /install_tmp/VMware-horizonagent-linux-x86_64-YYMM-y.y.y-xxxxxxxi/resources/
   vhci/patch/vhci.patch
   ```

Table 3-14. Compile and Install the USB VHCI Driver

Linux Distribution	Steps to Compile and Install USB VHCI Driver

Ubuntu	1 Install the dependency packages.
	`sudo apt-get install make`
	`sudo apt-get install gcc`
	`sudo apt-get install libelf-dev`
	2 (Ubuntu 22.04) Install the kernel header files.
	`sudo apt-get install linux-headers-$(uname -r)`
	3 Compile and install the VHCI driver.
	`tar -xzvf vhci-hcd-1.15.tar.gz`
	`cd vhci-hcd-1.15`
	`patch -p1 < full-path_to_patch-file`
	`make clean && make && sudo make install`
	4 If you have enabled the Extensible Firmware Interface (EFI) and UEFI Secure Boot on the virtual machine, configure signing settings for the VHCI driver.
	a Create an SSL key pair for the VHCI driver.
	`openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER`
	`-out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/" -addext`
	`extendedKeyUsage=1.3.6.1.5.5.7.3.3`
	b Sign the VHCI driver.
	`sudo /usr/src/linux-headers-$(uname -r)/scripts/sign-file sha256 ./`
	`MOK.priv ./MOK.der /lib/modules/$(uname -r)/kernel/drivers/usb/host/usb-`
	`vhci-iocifc.ko`
	
	`sudo /usr/src/linux-headers-$(uname -r)/scripts/sign-file sha256 ./`
	`MOK.priv ./MOK.der /lib/modules/$(uname -r)/kernel/drivers/usb/host/usb-`
	`vhci-hcd.ko`
	c Register the key for UEFI Secure Boot.
	`sudo mokutil --import MOK.der`
	Note This command issues a request to set a Machine Owner Key (MOK) password for UEFI Secure Boot.
	d To set up UEFI Secure Boot in the vSphere console, reboot the system. For more information, see https://sourceware.org/systemtap/wiki/SecureBoot.

Debian	1 Install the dependency packages.
	`sudo  apt install -y  patch g++ make linux-headers-$(uname -r)`
	2 Compile and install the VHCI driver.
	`tar -xzvf vhci-hcd-1.15.tar.gz`
	`cd vhci-hcd-1.15`
	`patch -p1 < full-path_to_patch-file`
	`mkdir -p linux/$(echo $(uname -r) | cut -d '-' -f 1)/drivers/usb/core`

Table 3-14. Compile and Install the USB VHCI Driver (continued)

<table>
<tr><th>Linux Distribution</th><th>Steps to Compile and Install USB VHCI Driver</th></tr>
<tr><td></td><td>cp /lib/modules/$(uname -r)/source/include/linux/usb/hcd.h linux/$(echo $(uname -r) | cut -d '-' -f 1)/drivers/usb/core

make clean && make && sudo make install</td></tr>
</table>

Table 3-14. Compile and Install the USB VHCI Driver (continued)

<table>
<tr><th>Linux Distribution</th><th>Steps to Compile and Install USB VHCI Driver</th></tr>
<tr><td>RHEL/CentOS 7.x
RHEL 8.x/9.x
Rocky Linux 8.x/9.x</td><td>1 Install the dependency packages.
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
sudo yum install patch
sudo yum install elfutils-libelf-devel
2 Compile and install the VHCI driver.
tar -xzvf vhci-hcd-1.15.tar.gz
cd vhci-hcd-1.15
patch -p1 < *full-path_to_patch-file*
make clean && make && sudo make install
3 (RHEL and Rocky Linux 9.x/8.x) To ensure that the VHCI driver works properly with USB redirection, configure signing settings for the driver.
a Create an SSL key pair for the VHCI driver.
openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER -out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/" -addext extendedKeyUsage=1.3.6.1.5.5.7.3.3
b Sign the VHCI driver.
sudo /usr/src/kernels/$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/$(uname -r)/kernel/drivers/usb/host/usb-vhci-iocifc.ko
sudo /usr/src/kernels/$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/$(uname -r)/kernel/drivers/usb/host/usb-vhci-hcd.ko
c Register the key for UEFI Secure Boot.
sudo mokutil --import MOK.der
Note This command issues a request to set a Machine Owner Key (MOK) password for UEFI Secure Boot.
d To set up UEFI Secure Boot in the vSphere console, reboot the system. For more information, see https://sourceware.org/systemtap/wiki/SecureBoot.</td></tr>
<tr><td>SLED/SLES</td><td>1 Find the version of the current kernel package.
rpm -qa | grep kernel-default-$(echo $(uname -r) | cut -d '-' -f 1,2)
The output is the name of the kernel package currently installed. If, for example, the package name is kernel-default-3.0.101-63.1, then the current kernel package version is 3.0.101-63.1.
2 Install the kernel-devel, kernel-default-devel, kernel-macros, and the patch packages.
sudo zypper install --oldpackage kernel-devel-*<kernel-package-version>* \
kernel-default-devel-*<kernel-package-version>* kernel-macros-*<kernel-package-version>* patch</td></tr>
</table>

Table 3-14. Compile and Install the USB VHCI Driver (continued)

<table>
<tr><th>Linux Distribution</th><th>Steps to Compile and Install USB VHCI Driver</th></tr>
<tr><td></td><td>

For example:

```
sudo zypper install --oldpackage kernel-devel-4.4.21-90.1 kernel-default-
devel-4.4.21-90.1 kernel-macros-4.4.21-90.1 patch
```

3 Compile and install the VHCI driver.

```
tar -xzvf vhci-hcd-1.15.tar.gz
cd vhci-hcd-1.15
patch -p1 < full-path_to_patch-file
mkdir -p linux/$(echo $(uname -r) | cut -d '-' -f 1)/drivers/usb/core
cp /lib/modules/$(uname -r)/source/include/linux/usb/hcd.h linux/$(echo $
(uname -r) | cut -d '-' -f 1)/drivers/usb/core
make clean && make && sudo make install
```

4 To ensure that the VHCI driver works properly with USB redirection, configure signing settings for the driver.

a Create an SSL key pair for the VHCI driver.

```
openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER
-out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/" -addext
extendedKeyUsage=1.3.6.1.5.5.7.3.3
```

b Find the path to the signing file for the VHCI driver.

```
sudo find / -name sign-file
```

This command returns the paths to all the signing files located on the system. The signing file path for the VHCI driver resembles the following example.

```
/usr/src/linux-5.3.18-24.9-obj/x86_64/default/scripts/
```

c Sign the VHCI driver. In the following commands, *<sign-file-path>* is the path to the signing file that you found earlier in step 4b.

```
sudo /<sign-file-path>/sign-file sha256 ./MOK.priv ./MOK.der /lib/
modules/$(uname -r)/kernel/drivers/usb/host/usb-vhci-iocifc.ko
sudo /<sign-file-path>/src/kernels/$(uname -r)/scripts/sign-file
sha256 ./MOK.priv ./MOK.der /lib/modules/$(uname -r)/kernel/drivers/usb/
host/usb-vhci-hcd.ko
```

d Register the key for UEFI Secure Boot.

```
sudo mokutil --import MOK.der
```

Note This command issues a request to set a Machine Owner Key (MOK) password for UEFI Secure Boot.

e To set up UEFI Secure Boot in the vSphere console, reboot the system. For more information, see https://sourceware.org/systemtap/wiki/SecureBoot.

</td></tr>
</table>

In addition, follow these guidelines:

- If your Linux kernel changes to a new version, you must recompile and reinstall the VHCI driver, but you do not need to reinstall Horizon Agent for Linux.

- You can also add Dynamic Kernel Module Support (DKMS) to the VHCI driver using steps similar to the following example for an Ubuntu system.

  a Install the kernel headers.

  ```
  sudo apt install linux-headers-`uname -r`
  ```

  b Install `dkms` using the following command.

  ```
  sudo apt install dkms
  ```

  c Extract and patch the VHCI TAR file.

  ```
  tar xzvf vhci-hcd-1.15.tar.gz
  cd vhci-hcd-1.15
  patch -p1 <full-path_to_patch-file>
  cd ..
  ```

  d Copy the extracted VHCI source files to the `/usr/src` directory.

  ```
  sudo cp -r vhci-hcd-1.15 /usr/src/usb-vhci-hcd-1.15
  ```

  e Create a file named `dkms.conf` and place it in the `/usr/src/usb-vhci-hcd-1.15` directory.

  ```
  sudo touch /usr/src/usb-vhci-hcd-1.15/dkms.conf
  ```

  f Add the following contents to the `dkms.conf` file.

  ```
  PACKAGE_NAME="usb-vhci-hcd"
  PACKAGE_VERSION=1.15
  MAKE_CMD_TMPL="make KVERSION=$kernelver"

  CLEAN="$MAKE_CMD_TMPL clean"

  BUILT_MODULE_NAME[0]="usb-vhci-iocifc"
  DEST_MODULE_LOCATION[0]="/kernel/drivers/usb/host"
  MAKE[0]="$MAKE_CMD_TMPL"

  BUILT_MODULE_NAME[1]="usb-vhci-hcd"
  DEST_MODULE_LOCATION[1]="/kernel/drivers/usb/host"
  MAKE[1]="$MAKE_CMD_TMPL"

  AUTOINSTALL="YES"
  ```

  g Add this VHCI driver in `dkms`.

  ```
  sudo dkms add usb-vhci-hcd/1.15
  ```

  h Build the VHCI driver.

  ```
  sudo dkms build usb-vhci-hcd/1.15
  ```

i Install the VHCI driver.

```
sudo dkms install usb-vhci-hcd/1.15
```

Virtual Machine Settings for 2D Graphics

When you create certain Linux virtual machines for a Horizon 8 deployment, you must change the vCPU and virtual memory settings for performance requirements.

Virtual machines that are configured to use NVIDIA GRID vGPU use the NVIDIA virtual graphics card, which is based on the NVIDIA physical graphics accelerator. You do not need to change the vCPU and virtual memory settings for these virtual machines.

Virtual machines that are configured to use 2D graphics use the VMware virtual graphics card, and you must change vCPU and virtual memory settings to improve the desktop performance. Use the following guidelines:

- For improved performance of a 2D desktop, set more vCPUs and virtual memory for the Linux virtual machine. For example, set 2 vCPUs and 2 GB of virtual memory.
- For the large screen display of multiple monitors, such as four monitors, set 4 vCPUs and 4 GB of virtual memory for the virtual machine.
- For improved video playback in a 2D desktop, set 4 vCPUs and 4 GB of virtual memory for the virtual machine.

Create a Virtual Machine and Install Linux

To prepare for a deployment of Linux remote desktops, start by using vSphere Client to create a virtual machine (VM) in vCenter Server. Then install your Linux distribution on the VM.

Prerequisites

- Verify that your deployment meets the requirements for supporting Linux desktops. See System Requirements for Horizon Agent for Linux.
- Familiarize yourself with the video memory (vRAM) settings requirements for the monitors you plan to use with the VM. See Virtual Machine Settings for 2D Graphics.
- Familiarize yourself with the custom configuration parameters for VMs. See Virtual Machine Custom Configuration Parameters.

- Verify that an ISO image file of the guest Linux distribution is in a datastore on your ESXi server.

  Note When selecting a guest Linux distribution, consider the following limitations for instant-clone desktop pools and multi-session hosts.

  Horizon Agent for Linux only supports instant-clone desktop pools created from virtual machines running the following operating systems:

  - Ubuntu 20.04/22.04
  - Debian 10.x/11.x/12.x
  - RHEL 7.9/8.x/9.x
  - Rocky Linux 8.x/9.x
  - CentOS 7.9
  - SLED/SLES 15.x

  Only virtual machines running RHEL Workstation 7.9/8.x/9.x, Rocky Linux 8.x/9.x, Ubuntu 20.04/22.04, or Debian 10.x/11.x/12.x can support multi-session published desktop pools and single-session or multi-session application pools.

Procedure

You can create a VM in vSphere from scratch or by cloning an existing VM. This procedure describes creating a VM from scratch.

1. Log in to vSphere Client.
2. Right-click any inventory object that is a valid main object of a VM, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**.
3. Select **Create a new virtual machine** and click **Next**.
4. Specify the number of vCPUs and the vMemory size. For the required settings, refer to the following guidelines.
   - If you are preparing the VM for deployment as a single-session virtual desktop pool, follow the guidelines in the installation guide for your Linux distribution.
   - If you are preparing the VM to serve as a multi-session host for a published desktop or application pool, specify at least 8 vCPUs and 40 GB of vMemory.

     Important A minimum of 8 vCPUs and 40 GB of vMemory is required to support up to 50 user sessions per published desktop or published application.
5. On the **Customize hardware** page, select **Virtual Hardware** to configure hardware settings.

   a Click **Add New Device** and select a CD/DVD drive. Set the media type to use an ISO image file, select the ISO image file of the guest Linux distribution that you placed in a datastore on your ESXi server. Then select **Connect at power on**.

6 On the **Customize hardware** page, select **VM Options** to configure VM settings.

   a **(Optional)** In the **Boot Options**, set **Boot Delay** to 10,000 milliseconds.

   You can set the boot delay to easily access the VM's BIOS on boot and modify the system settings. After you modify the system settings, you can reset the boot delay.

7 For detailed information about other custom options, see Virtual Machine Custom Configuration Parameters. After configuring the VM options, Click **Finish** to create the VM.

8 Power on the VM and install the Linux distribution from the ISO image that you specified earlier.

   a In vSphere Client, right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

      Because you configured the CD/DVD drive to point to the ISO image of the guest distribution and to connect at power on, the guest distribution installation process begins automatically.

   b Click the **Console** tab and follow the instructions in the guest distribution installers.

   Important Always use a VM equipped with a freshly installed Linux operating system as the golden image of an instant-clone desktop pool. Do not use an already cloned system as the golden image VM.

9 Configure the desktop environment to use for the specific Linux distribution.

   For more information, see Desktop Environment.

10 Ensure that the VM hostname is resolvable to 127.0.0.1.

11 Proceed to Prepare a Linux Machine for Remote Desktop Deployment.

Virtual Machine Custom Configuration Parameters

You can use virtual machine custom configuration parameters as baseline settings when you create a virtual machine for remote desktop deployment.

Table 3-15. Custom Configuration Parameters

Parameter	Description and Recommendations
`Name and Folder`	The name and location of the virtual machine. If you plan to use the virtual machine as a template, assign a generic name. The location can be any folder within your data center inventory.
`Host/Cluster`	The ESXi server or cluster of server resources that will run the virtual machine. If you plan to use the virtual machine as a template, the location of the initial virtual machine does not necessarily specify where future virtual machines created from template will reside.
`Resource Pool`	If the physical ESXi server resources are divided into resource pools, you can assign them to the virtual machine.
`Datastore`	The location of files associated with the virtual machine.

Table 3-15. Custom Configuration Parameters (continued)

Parameter	Description and Recommendations
`Hardware Machine Version`	The hardware machine version that is available depends on the ESXi version you are running. As a best practice, select the latest available hardware machine version, which provides the greatest virtual machine functionality. Certain VMware Horizon 8 features require minimum hardware machine versions.
`Guest Operating System`	The type of operating system that you will install in the virtual machine.
`CPUs`	The number of virtual processors in the virtual machine.
`Memory`	The amount of memory to allocate to the virtual machine.
`Network`	The number of virtual network adapters (NICs) in the virtual machine. One NIC is usually sufficient. The network name should be consistent across virtual infrastructures. An incorrect network name in a template can cause failures during the instance customization phases. When you install Horizon Agent on a virtual machine that has more than one NIC, you must configure the subnet that Horizon Agent uses. See Configure a Virtual Machine with Multiple NICs for Horizon Agent for more information.
`SCSI Controller`	The type of SCSI adapter to use with the virtual machine. Select either LSI Logic SAS or VMware Paravirtual (PVSCSI). Using PVSCSI may require additional steps depending on the version of Windows to be installed. For more information, see the VMware Knowledge Base article Configuring disks to use VMware Paravirtual SCSI (PVSCSI) controllers (1010398).
`Select a Disk`	The disk to use with the virtual machine. Create a new virtual disk based on the amount of local storage that you decide to allocate to each user. Allow enough storage space for the OS installation, patches, and locally installed applications. To reduce the need for disk space and management of local data, you should store the user's information, profile, and documents on network shares rather than on a local disk.

Prepare a Physical Linux Machine for Desktop Deployment

This page outlines the steps you must perform to prepare a physical Linux machine for use in a desktop pool.

Prerequisites

- Verify that the physical machine is running a supported version of RHEL 8.x or 9.x, as described in Supported Linux Distributions for Horizon Agent. Horizon Agent is only supported on physical machines running the RHEL distribution.
- To support software encoding in remote desktop sessions, verify that the physical machine is equipped with an NVIDIA GPU.

- To support hardware encoding in remote desktop sessions, verify that the physical machine is equipped with an NVIDIA GPU that supports all the following features:

  - NVIDIA Capture SDK, including the NVIDIA Framebuffer Capture (NVFBC) API
  - NVIDIA Encoder (NVENC)
  - H.264 hardware encoding

  For example, the following GPU models meet all the support requirements:

  - Tesla
  - Quadro K2000 and later
  - Quadro M2000 and later
  - Quadro P2000 and later
  - Quadro RTX2000 and later

  Horizon Agent needs the GPU to support H.264 for performance requirements, in addition to the hardware encoding method you want to use for the rendering of remote desktop sessions. For information about the capabilities of specific GPUs, including supported encoding methods, refer to https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new.

Procedure

1 Open a Secure Shell (SSH) connection to the physical Linux machine.

An SSH connection is recommended to perform Horizon Agent installation, upgrade, and uninstallation procedures on the machine. Alternatively, you can switch to a different console window (for example, press Ctrl+Alt+F3).

2 Ensure that the machine host name is resolvable to 127.0.0.1.

3 If you are upgrading an existing version of Horizon Agent on the machine, stop the `viewagent` service.

```
sudo systemctl stop viewagent
```

4 Stop the X server and Gnome Display Manager (GDM) on the machine.

```
sudo systemctl stop gdm
sudo systemctl isolate multi-user.target
```

5 Download and install Horizon Agent in unmanaged mode.

For detailed installation instructions, see Install Horizon Agent on a Linux Machine. For information on unmanaged mode, see Command-line Options for Installing Horizon Agent for Linux .

For example, the following commands can be used to install Horizon Agent in unmanaged mode.

- Tarball installer:

  ```
  sudo ./install_viewagent.sh -M no -b <broker address> -u <user> -p <password> -d
  <domain>
  ```

- RPM installer:

  ```
  sudo rpm -ivh VMware-horizonagent-linux-YYMM-y.y.y-xxxxxxx.el8.x86_64.rpm

  sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh -M no -b <broker address> -u <user> -p
  <password> -d <domain>
  ```

Note As an alternative to deploying the machine in unmanaged mode, you can configure the machine for direct connection using the Horizon Agent Direct-Connection Plug-In. For more information, see *Horizon Agent Direct-Connection Plug-In* on the VMware Horizon Documentation portal.

6. After completing the Horizon Agent installation, configure the following settings in the `/etc/vmware/config` file.

   ```
   Desktop.displayNumberMin=0
   Desktop.displayNumberMax=0
   ```

7. Restart the machine.

   Services that you stopped during the installation are resumed after the machine restarts.

8. Configure the desktop environment.

   For more information, see Desktop Environment.

9. Proceed to Prepare a Linux Machine for Remote Desktop Deployment.

Considerations for Physical Linux Machines

The following considerations apply to the physical machine after you install Horizon Agent.

- To display the graphical desktop on the physical machine, you must press Ctrl+Alt+F7. To configure a different function key shortcut, use the **DesktopWorker.ttyNum** option in `/etc/vmware/config`, as described in Edit Configuration Files on a Linux Desktop.
- If you add a monitor dynamically, you must restart the machine to detect the added monitor. Alternatively, you can reinstall Horizon Agent to enable detection of the added monitor.

Prepare a Linux Machine for Remote Desktop Deployment

You must perform certain tasks to prepare a Linux machine for use as a desktop in a VMware Horizon 8 deployment.

To prepare a Linux machine, you must enable communication between the machine and the Horizon Connection Server. You must configure networking on the Linux machine so that the Linux machine can ping the Connection Server instance using its FQDN (fully qualified domain name).

If you are preparing the Linux machine for use as a multi-session host for a published desktop or application pool, you must perform a few more preparation steps.

Prerequisites

- Verify that you have created a new virtual machine (VM) in vCenter Server and installed your guest Linux distribution on the machine. See Create a Virtual Machine and Install Linux.

  Note If you are preparing the Linux machine for use as a multi-session host, verify that one of the following required distributions is installed on the machine:

  - RHEL Workstation 7.9/8.x/9.x
  - Rocky Linux 8.x/9.x
  - Ubuntu 20.04/22.04
  - Debian 10.x/11.x/12.x

- Configure an Active Directory domain controller for your remote desktops. For more information, see the *Horizon 8 Installation and Upgrade* document on the VMware Horizon Documentation portal.
- To make sure that desktop users are added to the local Remote Desktop Users group of the virtual machine, create a restricted Remote Desktop Users group in Active Directory. For more information, see the *Horizon 8 Installation and Upgrade* document on the VMware Horizon Documentation portal.
- If you plan to configure 3D graphics rendering for desktop pools, familiarize yourself with the **Enable 3D Support** setting for virtual machines. On ESXi hosts, you can select options that determine how the 3D renderer is managed on the ESXi host. For details, see the *vSphere Virtual Machine Administration* document on the VMware vSphere Documentation portal.
- Familiarize yourself with the steps for configuring your Linux machine to be resolvable through DNS. These steps vary for the different Linux distributions and releases. For instructions, consult the documentation for your Linux distribution and release.

If you are preparing the Linux machine for deployment as an automated full-clone or instant-clone desktop pool or for inclusion in an automated instant-clone farm, you must also do the following:

- Verify that the virtual switch that the instant-clone VMs connect to has enough ports to support the expected number of VMs. Each network card on a VM requires one port.
- To support instant-clone desktop pools or farms, verify that you have added an instant-clone domain administrator in Horizon Console.

Procedure

1 Map the Linux machine's host name to 127.0.0.1 in the `/etc/hosts` file.

Usually, for RHEL, Rocky Linux, CentOS, SLES, and SLED, you must manually map the host name to 127.0.0.1 because it is not automatically mapped. For Ubuntu/Debian, this step is not necessary because the mapping is there by default.

Note If you change the Linux machine's host name after installing Horizon Agent, you must map the new host name to 127.0.0.1 in the `/etc/hosts` file. Otherwise, the old host name continues to be used.

2 Ensure that the Linux machine is synchronized to a reliable time source.

Guests must use only one method of time synchronization.

In general, guests can use the VMware Tools time synchronization method in preference to other methods of time synchronization. The VMware Tools online help provides information on configuring time synchronization between guest and host.

Important Hosts that are being relied upon for time synchronization must themselves be synchronized to a reliable time source, using the built-in NTP client. Verify that all hosts in a cluster use the same time source.

Note Domain controllers can use either VMware Tools time synchronization or another reliable time source. All domain controllers within a forest and domain controllers across forests with inter-forest trusts must be configured to use the same time source.

3 Install service packs and updates to the guest Linux distribution.

4 Install antivirus software on the Linux machine.

5 Verify that Open VMware Tools (OVT) is installed on the machine. If needed, manually install OVT on the machine. For example, you can use the following installation command for Ubuntu/Debian machines:

```
sudo apt-get install open-vm-tools
```

6 Install other required software, such as smart card drivers if you are using smart card authentication.

7 If a proxy server is used in your network environment, configure network proxy settings.

8 Configure network connection properties.

a Assign a static IP address or specify that an IP address is assigned by a DHCP server.

VMware Horizon 8 does not support link-local (169.254.x.x) addresses for Horizon 8 desktops.

b Set the preferred and alternate DNS server addresses to your Active Directory server address.

9 To prepare the Linux machine for use in an automated instant-clone farm, in vSphere Client, deactivate the vApp Options setting on the virtual machine.

10 (RHEL, Rocky Linux, and CentOS only) Verify that `virbr0` is deactivated.

```
sudo virsh net-destroy default
sudo virsh net-undefine default
sudo service libvirtd restart
```

11 Ensure that the Horizon Connection Server instances in the pod can be resolved through DNS.

12 Configure the Linux machine to run in graphical mode by default.

For example, the following command configures a CentOS machine to run in graphical mode.

```
sudo systemctl set-default graphical.target
```

13 (Ubuntu/Debian only) If the machine is configured to authenticate with an OpenLDAP server, set the FQDN on the machine.

This step ensures that the information can be displayed correctly in the User field on the Sessions page in Horizon Console. Edit the `/etc/hosts` file as follows:

a `# nano /etc/hosts`

b Add the FQDN. For example: `127.0.0.1 hostname.domainname hostname`.

c Exit and save the file.

14 (SLED/SLES only) Deactivate **Change Hostname via DHCP**. Then set the static hostname and domain name.

a In Yast, click **Network Settings**.

b Click the **Hostname/DNS** tab.

c Deselect **Change Hostname via DHCP**.

d Enter the hostname and the domain name.

e Click **OK**.

15 To prepare a virtual machine for use as a multi-session host in a farm, install the required software packages.

- For RHEL Workstation:

```
sudo yum install http://mirror.centos.org/centos/7/os/x86_64/Packages/
cpptest-1.1.1-9.el7.x86_64.rpm
sudo yum install https://rpmfind.net/linux/centos/7.8.2003/os/x86_64/Packages/
uriparser-0.7.5-10.el7.x86_64.rpm
```

- For Ubuntu/Debian:

```
sudo apt-get install liburiparser1
```

16 Install Horizon Agent on the machine, as described in Install Horizon Agent on a Linux Machine. Ensure that you include the appropriate parameters in the installation script to install or enable required features, as described in Command-line Options for Installing Horizon Agent for Linux . For example:

- To prepare the virtual machine for inclusion in an automated instant-clone farm, use the following installation script:

  ```
  sudo ./install_viewagent.sh --multiple-session
  ```

- To prepare the virtual machine for inclusion in a manual farm, use the following installation script:

  ```
  sudo ./install_viewagent.sh --multiple-session -M no
  ```

17 To prepare the golden-image virtual machine for an instant-clone floating desktop pool or automated instant-clone farm, use vSphere Client to take a snapshot of the virtual machine in its powered-down state. This snapshot is used as the baseline configuration for the first set of instant-clone machines that are anchored to the virtual machine.

For more information, see "Take a Snapshot in the VMware Host Client" in *vSphere Single Host Management - VMware Host Client*, available from VMware vSphere Documentation.

Important Before you take a snapshot, completely shut down the golden-image virtual machine by using the shutdown or power-off command in the Linux operating system.

Install Linux Dependency Packages for Horizon Agent

Horizon Agent for Linux has some dependency packages unique to a Linux distribution. You must install these packages before installing Horizon Agent for Linux.

Prerequisites

Verify that a new virtual machine (VM) is created in vCenter Server and your Linux distribution is installed on the machine.

Procedure

- Install the mandatory packages that are not installed or upgraded by default. If any package does not meet the requirement, the installer breaks the installation.

Table 3-16. Mandatory Dependency Packages

Linux Distribution	Packages

RHEL 7.x/8.x and Rocky Linux 8.x	Install the `libappindicator-gtk3` package.
	`sudo yum install libappindicator-gtk3`
	Note If the `yum` command does not work, you can try the `dnf` package manager instead.
	`sudo dnf install libappindicator-gtk3`

RHEL and Rocky Linux 9.x	Perform one of the following installations.
	■ To install the `libappindicator-gtk3` package and also enable the Extra Packages for Enterprise Linux (EPEL), run the following commands.
	`sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm`
	`yum install libappindicator-gtk3`
	■ To install the `libappindicator-gtk3` package without enabling EPEL, run the commands shown in the following example.
	Note The package version numbers shown in the following example might differ from the actual versions provided at `https://dl.fedoraproject.org/pub/epel/9/`. Where applicable, replace the example version numbers with the actual version numbers.
	`sudo yum install https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/Packages/l/libdbusmenu-16.04.0-19.el9.x86_64.rpm`
	`sudo yum install https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/Packages/l/libdbusmenu-gtk3-16.04.0-19.el9.x86_64.rpm`
	`sudo yum install https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/Packages/l/libindicator-gtk3-12.10.1-22.el9.x86_64.rpm`
	`sudo yum install https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/Packages/l/libappindicator-gtk3-12.10.0-33.el9.x86_64.rpm`

Debian	`sudo apt-get install -y gnome-shell-extension-appindicator`

Upgrade the Operating System of a Linux Virtual Machine

This procedure explains how to upgrade the operating system of a Linux virtual machine (VM) that has Horizon Agent installed on it. Always follow the order of steps in this procedure when you want to upgrade your Linux VM to a new operating system version.

Prerequisites

Before starting the upgrade procedure, take a snapshot of the current Linux VM.

Procedure

1. Uninstall Horizon Agent from the VM.

   See Uninstall Horizon Agent From a Linux Machine.

2. Upgrade the operating system of the VM, following the upgrade steps for your Linux distribution.

   You can perform the upgrade using the graphical installation interface or installation commands for your Linux distribution.

3. Reinstall Horizon Agent on the VM.

   See Install Horizon Agent on a Linux Machine.

Configuring Session Collaboration on Linux Desktops

With the Session Collaboration feature, users can invite other users to join an existing Linux remote desktop session.

System Requirements for Session Collaboration

To support the Session Collaboration feature on Linux desktops, your VMware Horizon 8 deployment must meet certain requirements.

Table 3-17. System Requirements for Session Collaboration

Component	Requirements
Linux remote desktops	The Session Collaboration feature is supported on remote desktops running the following Linux distributions and desktop environments: ■ Ubuntu 20.04/22.04 with Gnome Ubuntu or MATE desktop environment ■ Debian 10.x/11.x/12.x with Gnome desktop environment ■ RHEL 7.9/8.x/9.x with Gnome Classic desktop environment ■ RHEL 7.9 with KDE desktop environment ■ Rocky Linux 8.x/9.x with Gnome desktop environment
Horizon Connection Server	The Horizon Connection Server instance uses an Enterprise license.
Display protocol	VMware Blast

Note RHEL 9.x/8.x, Rocky Linux, and Debian desktops require more system configuration to enable Session Collaboration. For more information, see the following sections.

For information about how to use the Session Collaboration feature, see the Horizon Client documentation.

Enabling Session Collaboration on a RHEL or Rocky Linux 9.x Desktop

For RHEL 9.x and Rocky Linux 9.x desktops, you must install the `libappindicator-gtk3` package and install the required GNOME Shell extension.

To enable the Session Collaboration feature and make the Session Collaboration icon available on a RHEL 9.x or Rocky Linux 9.x desktop, complete the following procedure.

1 To install the `libappindicator-gtk3` package, perform the installation procedure described in Install Linux Dependency Packages for Horizon Agent.

2 To enable AppIndicator support, download the required GNOME shell extension to the system.

   a Download the GNOME shell extension from https://extensions.gnome.org/extension/615/appindicator-support/. Select **40** for the shell version and **42** for the extension version.

   b Extract the contents of the downloaded package and rename the extension directory as `appindicatorsupport@rgcjonas.gmail.com` (the "uuid" value in the `metadata.json` file in the package).

   c Use the `mv` command to move the `appindicatorsupport@rgcjonas.gmail.com` extension directory to this location: `/usr/share/gnome-shell/extensions`.

   By default, the `appindicatorsupport@rgcjonas.gmail.com` extension is only readable to the root user. To support Session Collaboration, you must make this extension readable to other users as well.

3 Make the `metadata.json` file in the `appindicatorsupport@rgcjonas.gmail.com` directory readable to all users.

```
sudo chmod a+r metadata.json
```

Proceed to the next step of this procedure, based on your desktop pool type.

- If you are configuring an automated full-clone desktop pool, go to step 4.
- If you are configuring any other type of desktop pool, go to step 5.

4 (For automated full-clone desktop pools) Make the `appindicatorsupport@rgcjonas.gmail.com` extension readable to all users.

   a Open the extension configuration file for editing.

```
sudo vi /etc/dconf/db/local.d/00-extensions
```

   b Modify the configuration file to include `appindicatorsupport@rgcjonas.gmail.com` in the `enabled-extensions` list, as shown in the following example.

```
# List all extensions that you want to have enabled for all users
enabled-extensions=['background-logo@fedorahosted.org' ,
'appindicatorsupport@rgcjonas.gmail.com']
```

c Run the following sequence of commands.

```
sudo chmod 755 /etc/dconf/db/local.d/00-extensions
sudo dconf update
```

The session collaboration feature is now enabled for the desktop. You can skip the remaining steps of this procedure.

5 (For desktop pools besides automated full-clone) Make the appindicatorsupport@rgcjonas.gmail.com extension readable to the logged-in user.

a Install gnome-extensions-app.

b In the desktop environment, restart GNOME Shell by pressing the following sequence of keys on the keyboard.

```
Alt+F2
r
Enter
```

c In the desktop environment, run gnome-extensions-app and then enable **AppIndicator and KStatusNotifierItem Support**.

The session collaboration feature is now enabled for the desktop.

Enabling Session Collaboration on a RHEL or Rocky Linux 8.x Desktop

For RHEL 8.x and Rocky Linux 8.x desktops, you must install the required GNOME Shell extension to enable AppIndicator support.

1 Download the required GNOME shell extension to the system from https://extensions.gnome.org/extension/615/appindicator-support/. Select **3.32** for the shell version and **29** for the extension version.

2 Extract the contents of the downloaded package and rename the directory as appindicatorsupport@rgcjonas.gmail.com (the "uuid" value in the metadata.json file in the package).

3 Use the mv command to move the appindicatorsupport@rgcjonas.gmail.com directory to this location: /usr/share/gnome-shell/extensions.

By default, the metadata.json file in the appindicatorsupport@rgcjonas.gmail.com directory is only readable to the root user. To support Session Collaboration, you must make this file readable to other users as well.

4 Run the command to make metadata.json readable to other users, as shown in the following example.

```
sudo chmod a+r metadata.json
```

Proceed to the next step of this procedure, based on your desktop pool type.

- If you are configuring an automated full-clone desktop pool, go to step 5.

- If you are configuring any other type of desktop pool, go to step 6.

5 (For automated full-clone desktop pools) Make the `appindicatorsupport@rgcjonas.gmail.com` extension readable to all users.

   a Open the extension configuration file for editing.

   ```
   sudo vi /etc/dconf/db/local.d/00-extensions
   ```

   b Modify the configuration file to include `appindicatorsupport@rgcjonas.gmail.com` in the `enabled-extensions` list, as shown in the following example.

   ```
   # List all extensions that you want to have enabled for all users
   enabled-extensions=['appindicatorsupport@rgcjonas.gmail.com']
   ```

   c Run the following sequence of commands.

   ```
   sudo chmod 755 /etc/dconf/db/local.d/00-extensions
   sudo dconf update
   ```

   The session collaboration feature is now enabled for the desktop. You can skip the remaining steps of this procedure.

6 (For desktop pools besides automated full-clone) Make the `appindicatorsupport@rgcjonas.gmail.com` extension readable to the logged-in user.

   a Install `gnome-tweaks`.

   b In the desktop environment, restart GNOME Shell by pressing the following sequence of keys on the keyboard.

   ```
   Alt+F2
   r
   Enter
   ```

   c In the desktop environment, run `gnome-tweaks` and then enable **KStatusNotifierItem/AppIndicator Support**.

   The session collaboration feature is now enabled for the desktop.

Enabling Session Collaboration on a Debian 11.x/12.x Desktop

To enable the Session Collaboration feature on a Debian 11.x/12.x desktop, complete the following procedure.

1 Install `gnome-shell-extension-appindicator`.

```
sudo apt-get install -y gnome-shell-extension-appindicator
```

2 Open the Extensions window.

```
gnome-extensions-app
```

3 In the Extensions window, enable **Ubuntu AppIndicators**.

Enabling Session Collaboration on a Debian 10.x Desktop

To enable the Session Collaboration feature on a Debian 10.x desktop, complete the following procedure.

1 Install `gnome-shell-extension-appindicator`.

```
sudo apt-get install -y gnome-shell-extension-appindicator
```

2 Open the Extensions window.

```
gnome-tweaks
```

3 In the Extensions window, enable **Kstatusnotifieritem/appindicator support**.

Setting Session Collaboration Options in Configuration Files

Set the following option in the `/etc/vmware/viewagent-custom.conf` file to enable or deactivate the Session Collaboration feature.

- `CollaborationEnable`

Set the following options in the `/etc/vmware/config` file to configure the settings used during a collaboration session.

- `collaboration.logLevel`
- `collaboration.maxCollabors`
- `collaboration.enableEmail`
- `collaboration.serverUrl`
- `collaboration.enableControlPassing`

See Edit Configuration Files on a Linux Desktop for more information.

Session Collaboration Feature Limitations

The following general limitations apply to the Session Collaboration feature:

- Users cannot use the following remote desktop features in a collaboration session.
  - USB redirection
  - Audio input redirection
  - Client drive redirection
  - Smart card redirection
  - Clipboard redirection
- Users cannot change the remote desktop resolution in a collaboration session.
- Users cannot have multiple collaboration sessions on the same client machine.

Troubleshooting Issues with Session Collaboration

Use the following remedies to troubleshoot issues related to Session Collaboration.

- (RHEL and Rocky Linux 9.x) If the Session Collaboration icon fails to appear in the system tray, perform the configuration steps described in Enabling Session Collaboration on a RHEL or Rocky Linux 9.x Desktop.
- If the Session Collaboration icon fails to appear in the system tray after a user logs in for the first time to the remote desktop, instruct the user to try one of the following remedies.
  - Disconnect from and reconnect to the desktop. The Session Collaboration icon usually appears after reconnection to the desktop.
  - Restart GNOME Shell using the following steps.
    1. Press Alt+F2 to display the **Run a Command** dialog box.
    2. Type "r" in the dialog box.
    3. Press Enter.
- If the Session Collaboration icon in the system tray is unresponsive after a user logs in for the first time to the remote desktop, instruct the user to resize the remote desktop window. The Session Collaboration icon becomes responsive after the desktop window is resized.

Configure a Golden Image Linux VM for Instant Clones

After creating a Linux virtual machine (VM) that you plan to use as the golden image for an instant-clone desktop pool, you must configure the machine environment.

Horizon Agent for Linux only supports instant-clone desktop pools created from virtual machines running the following operating systems:

- Ubuntu 20.04/22.04
- Debian 10.x/11.x/12.x
- RHEL 7.9/8.x/9.x
- Rocky Linux 8.x/9.x
- CentOS 7.9

- SLED/SLES 15.x

Note For Linux desktops, vGPU graphics capabilities are only supported on instant-clone pools created from machines running the following distributions:

- Ubuntu 20.04/22.04
- Debian 10.x
- RHEL 7.9/8.x/9.x
- Rocky Linux 8.x/9.x
- CentOS 7.9

Note The VMware Horizon 8 compute profile feature significantly improves golden image management and reduces the number of golden images required to create desktop pools for different requirements.

Prerequisites

- Verify that the system disk contains a single volume.
- Verify that the virtual machine does not contain an independent disk. However, the golden image virtual machine can contain multiple disks.

  An independent disk is excluded when you take a snapshot of the virtual machine. Clones are based on a snapshot and therefore will not contain the independent disk.
- Turn off the hibernation option to reduce the size of each clone's virtual disk.
- In vSphere Client, deactivate the vApp Options setting on the golden image virtual machine.
- Turn off the HotPlug capability on removable devices. See KB 1012225.

Procedure

1. Create a Linux virtual machine (VM) and perform a fresh installation of an operating system that supports the creation of instant-clone desktop pools. See the list of supported operating systems earlier on this page.

   For more information, see Create a Virtual Machine and Install Linux.

   Important Always use a VM equipped with a freshly installed Linux operating system as the golden image VM of an instant-clone desktop pool. Do not use an already cloned system as the golden image VM.
2. Complete the preparation steps described in Prepare a Linux Machine for Remote Desktop Deployment.
3. Install Horizon Agent for Linux on the Linux VM. See Install Horizon Agent on a Linux Machine.

4 Integrate your Linux VM with Active Directory. The golden image must belong to the same Active Directory domain as the domain that the desktop machines will join.

   - To use the SSSD solution, complete the procedure described in Configure SSSD Offline Domain Join for Linux Desktops.
   - To use Samba offline domain join, complete the procedure described in Configure Samba Offline Domain Join for Linux Desktops.
   - If you want to deactivate offline domain join, you must set the `OfflineJoinDomain` option to **`none`** in the `/etc/vmware/viewagent-custom.conf` file. Otherwise, the creation of the instant-clone floating desktop pool fails.

   Samba supports offline domain join with Active Directory for instant-cloned desktops running any Linux distribution supported by Horizon Agent. However, VMware recommends using SSSD Authentication for desktops running newer distributions and Samba only for desktops running older distributions, as described in the following note.

   Note

   - VMware recommends using the SSSD Authentication method (instead of Samba) for desktops running the following Linux distributions.
     - Ubuntu 20.04/22.04
     - Debian 11.x/12.x
     - RHEL 8.x/9.x
     - Rocky Linux 8.x/9.x
     - SLED/SLES 15.x
   - VMware recommends using the Samba method for desktops running the following Linux distributions.
     - Debian 10.x
     - RHEL/CentOS 7.9

5 If your DHCP server does not broadcast to a DNS server, specify a DNS server for your Linux system.

   A new virtual network adapter is added when a new instant-cloned VM is created. Any setting in the network adapter, such as the DNS server, in the VM template is lost when the new network adapter is added to the instant-cloned VM. PBIS requires a valid DNS server and the FQDN mapping in the `/etc/hosts` is not acceptable. To avoid losing the DNS Server setting when the new network adapter is added to the cloned VM, you must specify a DNS server on your Linux system.

   Note For best results, use NetworkManager instead of WICD for network management. WICD might produce problems when used with instant-cloned SLED/SLES 15.x VMs.

6. (Optional) If you want to add an NFS mount in the `/etc/fstab` file of the Linux golden image, use one of the following methods.

   - Add a 'soft' flag in `/etc/fstab`, such as:

     ```
     10.111.222.333:/share     /home/nfsmount    nfs
     rsize=8192,wsize=8192,timeo=14,soft,intr,tcp
     ```

   - If you do not want to use the 'soft' flag in `/etc/fstab`, you cannot configure the `/etc/fstab` in the Linux golden image. You can write a power-off script to configure the `/etc/fstab` file, and then specify this power-off script for the ClonePrep tool. For more information, see the *Horizon 8 Administration* document.

7. Shut down the Linux VM and create a golden image by creating a snapshot of your powered off Linux VM using vSphere Client.

   For more information, see "Take a Snapshot in the VMware Host Client" in *vSphere Single Host Management - VMware Host Client*, available from VMware vSphere Documentation.

Using ClonePrep to Customize Linux Desktops

ClonePrep is a VMware customization process run during instant clone deployment to personalize each desktop clone created from the parent image.

Important When you use ClonePrep power-off or post-synchronization scripts, ensure that the scripts are located in the `/var/userScript` folder, owned by the root user, and have the file permissions set to 700.

ClonePrep Processes

ClonePrep ensures that all instant clones join an Active Directory domain. The clones have the same computer security identifiers (SIDs) as the golden image. ClonePrep also preserves the globally unique identifiers (GUIDs) of applications, although some applications generate a new GUID during customization.

During the initial startup of each desktop, ClonePrep:

- Creates a new computer account in Active Directory for each desktop.
- Gives the instant clone desktop a new name.
- Joins the desktop to the appropriate domain.

The following table shows the effect of various ClonePrep operations on the security identifiers (SIDs) of instant clones.

	Creation	Push Image	On User Logout
ClonePrep	Parent Image's SID are used for the desktops	SIDs are preserved unless parent image is changed	SIDs are preserved unless parent image is changed

ClonePrep Guest Customization Scripts

When you add an instant-clone desktop pool, you can specify a script so that it runs immediately after a clone is created and another script to run before the clone is powered off.

Refer to the following guidelines when creating ClonePrep customization scripts.

- **Path to ClonePrep Scripts**

  You can specify the scripts when you create or edit the desktop pool. The scripts must reside on the golden image in the `/var/userScript` folder, be owned by the root user, and have the file permissions set to 700. You cannot use a UNC path to a network share.

- **ClonePrep Script Timeout Limit**

  By default, ClonePrep stops a script if the execution takes longer than 20 seconds. Alternatively, you can specify a script that runs another script or process that takes a long time to run.

- **ClonePrep Script Account**

  ClonePrep runs the scripts using the same account that the VMware Horizon 8 Instant Clone Agent service uses. Do not change this login account. If you do, the clones can fail to start.

Installing Horizon Agent for Linux

You must install Horizon Agent on a Linux virtual machine so that Horizon Connection Server can communicate with and manage the desktops based on that virtual machine.

Use the Easy Setup Tool to Prepare a Linux Machine

This page describes the Easy Setup Tool (`easyinstall_viewagent.sh`) for Linux machines. This tool performs all the installations and system configurations required to make a Linux machine available for use in a VMware Horizon 8 deployment.

Overview of the Easy Setup Tool

The Easy Setup Tool is a guided installer that performs the following operations on the Linux machine.

- **System pre-check**

  Validates that the machine meets the following requirements:

  - The machine is running a supported Linux distribution, as specified in Supported Linux Distributions for Horizon Agent.
  - The required software repository is correctly configured on the machine.
  - The machine is configured with a supported desktop environment, as specified in Desktop Environment.

  The tool displays a notification if the machine fails to meet a certain requirement.

- **System configurations**

  Performs the following system configurations:

  - Configures DNS.
  - Configures NTP and hostname settings and joins the machine to a specified Active Directory domain.

    Note This release of the Easy Setup Tool performs only the System Security Services Daemon (SSSD) Authentication method of domain join.

- **Horizon Agent installation**

  Performs the following operations on the machine:

  - Builds the following kernel modules to support certain features of Linux desktops:
    - V4L2Loopback driver, which supports Real-Time Audio-Video (RTAV)
    - USB VHCI driver, which supports USB redirection
  - Installs the mandatory agent dependencies, as listed in Install Linux Dependency Packages for Horizon Agent.
  - Installs Horizon Agent for Linux, with specified installation options.

Note For information on how to specify installation parameters such as the Active Directory domain, agent installation options, and the level of installer prompts, see Configuration Parameters for the Easy Setup Tool.

Download and Run the Easy Setup Tool

1. Download the Horizon Agent for Linux installer package from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Navigate to the download page for the current release ofVMware Horizon and then to the download page for VMware Horizon for 64-bit Linux.

   Download the Horizon Agent installer tarball with filename `VMware-horizonagent-linux-x86_64-YYMM-y.y.y-xxxxxxx.tar.gz`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxxx* is the build number.

2. Unpack the tarball for your Linux distribution. For example:

   ```
   tar -xvzf VMware-horizonagent-linux-x86_64-YYMM-y.y.y-xxxxxxx.tar.gz
   ```

3. Navigate to the tarball folder and run the `easyinstall.viewagent.sh` script as a root user. Append the command-line parameters for any installation options you want to include.

   For detailed information, see Command-line Parameters for the Easy Setup Tool.

Use the following command examples for reference:

```
#Run the Easy Setup Tool with default prompts and installation options
./easyinstall_viewagent.sh

#Run the tool in silent mode with installation options specified in easyinstall.conf
./easyinstall_viewagent.sh -s -f ./easyinstall.conf
```

4. Allow the Easy Setup Tool to proceed without interruption, and respond to any installer prompts as needed.

5. After the installation process is complete, restart the Linux machine to make the changes take effect.

6. Verify that the *viewagent* service is started by running the following command.

```
sudo service viewagent status
```

Command-line Parameters for the Easy Setup Tool

The following table describes the command-line parameters that you can append to the `./easyinstall_viewagent.sh` run command to specify installation options and prompt levels.

Option	Description
-s, --silent	Runs the Easy Setup Tool in silent mode bypassing all installer prompts. Required installation options are retrieved from the configuration file specified by the `-f` parameter. For more details, see Configuration Parameters for the Easy Setup Tool. Command example: `./easyinstall_viewagent.sh -s -f ./easyinstall.conf`
-l, --prompt-level	Specifies the level of user interaction based on the level of installer prompts. Settings for each prompt level are retrieved from the configuration file specified by the `-f` parameter. For more details, see Configuration Parameters for the Easy Setup Tool. Allowed values: ■ `default` - Displays only the prompts for basic installation options. When the `-l` parameter is not included or not configured, this `default` prompt level is used. ■ `advanced` - In addition to `default` prompts, displays prompts for advanced installation options such as whether to install remote experience features. ■ `expert` - In addition to `default` and `advanced` prompts, displays prompts for expert installation options such as whether to install FIPS support. Command example: `./easyinstall_viewagent.sh -l advanced -f ./easyinstall.conf`
-f, --config-file	Reads configurations from the specified configuration file. For more information, see Configuration Parameters for the Easy Setup Tool. Command example: `./easyinstall_viewagent.sh -s -f ./easyinstall.conf`
-p, --pre-check-only	Only performs the pre-check operations described in Overview of the Easy Setup Tool. Does not perform system configurations or Horizon Agent installation. Command example: `./easyinstall_viewagent.sh -p`
-c, --configure-only	Only performs the system configurations described in Overview of the Easy Setup Tool. Does not perform pre-check operations or Horizon Agent installation. Command example: `./easyinstall_viewagent.sh -c`

Option	Description
-i, --install-agent-only	Only installs Horizon Agent, as described in Overview of the Easy Setup Tool. Does not perform pre-check operations or system configurations. Command example: `./easyinstall_viewagent.sh -i`
-h, --help	Displays help information for the Easy Setup Tool, and exits the tool. Command example: `./easyinstall_viewagent.sh -h`

Configuration Parameters for the Easy Setup Tool

You can specify configuration parameters for the Easy Setup Tool by writing the parameters into a configuration file and then retrieving the file with the `-f` command-line parameter.

For example, the following command runs the tools with `advanced` installer prompts as specified in the `easyinstall.conf` configuration file.

```
./easyinstall_viewagent.sh -l advanced -f ./easyinstall.conf
```

Observe the following rules and conventions when writing a configuration file:

- Refer to the configuration template `easyinstall.conf.template`, located in the same tarball folder that contains the `easyinstall_viewagent.sh` script.
- Save your configuration file in the same tarball folder.
- Configuration parameters are grouped into sets corresponding to the three installer prompt levels: `default`, `advanced`, and `expert`.
- To bypass a prompt, comment out the configuration parameter for that prompt in the configuration file.
- In the following tables, entries labeled "Optional" correspond to prompts that accept optional input. Users can skip an optional prompt without entering any input.
- For prompts that accept "y" or "n" input, the capitalized setting represents the default setting.

  For example, the EASYINSTALL_AGENT_MANAGED parameter takes "Y" as its default setting, meaning that Horizon Agent is installed in managed mode by default. The default setting takes effect when bypassing a prompt or running the Easy Setup Tool in silent mode.

Table 3-18. Parameters for Default Prompt Level

Configuration Parameter	Description
EASYINSTALL_HOSTNAME	Specify the hostname for the host (Optional).
EASYINSTALL_DNS_LIST	Specify the DNS for the host (Optional).
EASYINSTALL_DOMAIN_FQDN	Specify the FQDN of the Active Directory domain to join.
EASYINSTALL_DOMAIN_JOIN_USER	Specify the user account to use for domain join.
EASYINSTALL_DOMAIN_JOIN_PASSWORD	Specify the password to use for domain join.
EASYINSTALL_PROXY	Specify the proxy server to use during the configuration process (Optional).
EASYINSTALL_AGENT_ACCEPT_GENERAL_TERMS	Specify whether to accept the General Terms agreement [Y/n]. You must accept the General Terms to proceed with the Easy Setup Tool.

Table 3-19. Parameters for Advanced Prompt Level

Configuration Name	Description
EASYINSTALL_NTP	Enter the IP address of the NTP server (Optional).
EASYINSTALL_DOMAIN_JOIN	Specify whether to join the Active Directory domain [Y/n].
EASYINSTALL_AGENT_MANAGED	Specify whether to install Horizon Agent in managed mode [Y/n].
EASYINSTALL_AGENT_MULTIPLE_SESSION	Specify whether to install support for multiple sessions [Y/n].
EASYINSTALL_AGENT_WEBCAM	Specify whether to install the webcam redirection feature [y/N].
EASYINSTALL_AGENT_AUDIO_IN	Specify whether to install support for audio input redirection [y/N].
EASYINSTALL_AGENT_USB_REDIRECTION	Specify whether to install the USB redirection feature [y/N].
EASYINSTALL_AGENT_CLIENT_DRIVE_REDIRECTION	Specify whether to install the client drive redirection feature [Y/n].
EASYINSTALL_AGENT_CLIPBOARD_REDIRECTION	Specify whether to install the clipboard redirection feature [Y/n].
EASYINSTALL_AGENT_PRINTER_REDIRECTION	Specify whether to install the printer redirection feature [Y/n].
EASYINSTALL_AGENT_SKIP_BUILD_MODULES	Specify whether to skip building required modules [y/N].

Table 3-19. Parameters for Advanced Prompt Level (continued)

Configuration Name	Description
EASYINSTALL_AGENT_SINGLE_SIGN_ON	Specify whether to install support for single sign-on [Y/n].
EASYINSTALL_AGENT_RESTART_AFTER_INSTALLATION	Specify whether to restart the machine automatically after the installation [y/N].
EASYINSTALL_HORIZON_CONNECTION_SERVER_ADDRESS	Enter the FQDN or IP address of the Connection Server (for unmanaged mode only).
EASYINSTALL_HORIZON_ADMIN_DOMAIN	Enter the administrator domain name of the Connection Server (for unmanaged mode only).
EASYINSTALL_HORIZON_ADMIN_USER	Enter the administrator name of the Connection Server (for unmanaged mode only).
EASYINSTALL_HORIZON_ADMIN_PASSWORD	Enter the administrator password of the Connection Server (for unmanaged mode only).

Table 3-20. Parameters for Expert Prompt Level

Configuration Name	Description
EASYINSTALL_AGENT_FIPS	Specify whether to install support for FIPS mode [y/N].
EASYINSTALL_AGENT_IPV6	Specify whether to install support for IPv6 networking [y/N].
EASYINSTALL_AGENT_NO_HOSTED_APP	Specify whether to disallow single-session application pools [y/N].
EASYINSTALL_AGENT_DISABLE_VMWGREETER	Specify whether to deactivate the VMware greeter, which supports the True SSO and smart card SSO features [y/N].
EASYINSTALL_AGENT_SMARTCARD_REDIRECTION	Specify whether to install the smartcard redirection feature [y/N].
EASYINSTALL_AGENT_TRUE_SSO	Specify whether to install the True SSO feature [y/N].
EASYINSTALL_AGENT_SELF_SIGNED_CERT_SUBJECT_DN	Enter the Subject DN of the preferred self-signed certificate (Optional).
EASYINSTALL_AGENT_JMS_SSL_KEYSTORE_PASSWORD	Enter the preferred JMS SSL keystore password (Optional).
EASYINSTALL_AGENT_VHCI_SOURCE_DOWNLOAD_PATH	Specify the file path of the VHCI source package (Optional).
EASYINSTALL_AGENT_V4L2LOOPBACK_SOURCE_DOWNLOAD_PATH	Specify the file path of the V4L2Loopback source package (Optional).
EASYINSTALL_HORIZON_ADMIN_KDC	Specify the Kerberos Key Distribution Center (KDC) for theVMware Horizon 8 administrator domain (Optional, for unmanaged mode only).

Table 3-20. Parameters for Expert Prompt Level (continued)

Configuration Name	Description
EASYINSTALL_HORIZON_CONNECTION_SERVER_KDC	Specify the KDC for the Connection Server domain (Optional, for unmanaged mode only).
EASYINSTALL_HORIZON_CONNECTION_SERVER_DOMAIN	Enter the domain name of the Connection Server (Optional, for unmanaged mode only).

Feature Considerations for the Easy Setup Tool

The following considerations and limitations apply to the Easy Setup Tool.

- SSSD Authentication is the only domain-join method currently supported by the tool.
- If the True SSO feature is installed, you must perform further configuration steps as described in Set Up True SSO for Linux Desktops.

  If the smart card redirection feature is installed, you must perform further configuration steps as described in Set Up Smart Card Redirection for Linux Desktops.
- If Secure Boot is enabled on the machine, you must sign both the VHCI driver (see VHCI Driver for USB Redirection) and V4L2Loopback driver (see Install the V4L2Loopback Driver on a Linux Machine.

Install Horizon Agent on a Linux Machine

This documentation page describes how to install Horizon Agent on a Linux machine. Installing Horizon Agent allows you to deploy the machine as a remote desktop.

Prerequisites

- Verify that the Linux machine is prepared for desktop use. See Prepare a Linux Machine for Remote Desktop Deployment.
- If you plan to install Horizon Agent using the tarball installer, review the optional parameters for the `install_viewagent.sh` setup script. See Command-line Options for Installing Horizon Agent for Linux .
- If you plan to install Horizon Agent on a virtual machine, open a Terminal window. You can run the Horizon Agent installation commands from the Terminal.
- If you plan to install Horizon Agent on a physical host machine, open a Secure Shell (SSH) connection to the machine. SSH is the recommended method for running Horizon Agent installation commands on a physical machine. In addition, stop the X server and Gnome Display Manager as described in Prepare a Physical Linux Machine for Desktop Deployment.

Horizon Agent Installer

The Horizon Agent installer is available in two different formats:

- The `.tar.gz` installer package supports installation on all Linux distributions. This installer is not digitally signed.
- The `.rpm` installer package supports installation on RHEL 8.x machines only. This installer is digitally signed.

If you are upgrading Horizon Agent from an existing version, see the instructions in Upgrade Horizon Agent on a Linux Machine.

Caution If you plan to use NVIDIA GRID vGPU, you must configure 3D graphics features on the Linux virtual machine before you install Horizon Agent. If you install Horizon Agent first, required parameters in the `xorg.conf` file are overwritten, and the 3D graphics features do not work.

See Chapter 5 Setting Up Graphics for Linux Virtual Machines. Install Horizon Agent after the 3D graphics configuration is completed.

For a 2D graphics configuration, you can install Horizon Agent after you complete the steps in Prepare a Linux Machine for Remote Desktop Deployment.

Install Horizon Agent Using the Unsigned Tarball Installer

Note For a RHEL 8.x machine, you also have the option to install Horizon Agent using a digitally signed installer. See the procedure described later in this article.

1. Download the Horizon Agent for Linux installer package from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Navigate to the download page for the current release ofVMware Horizon and then to the download page for VMware Horizon for 64-bit Linux.

   Download the Horizon Agent installer tarball with filename `VMware-horizonagent-linux-x86_64-`*`YYMM-y.y.y-xxxxxxx`*`.tar.gz`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxxx* is the build number.

2. Unpack the tarball for your Linux distribution. For example:

   ```
   tar -xvzf VMware-horizonagent-linux-x86_64-YYMM-y.y.y-xxxxxxx.tar.gz
   ```

3. To support certain features, install the required drivers as follows.

   - To support the USB Redirection feature, install the VHCI driver as described in VHCI Driver for USB Redirection.
   - To support the Real-Time Audio-Video feature, complete the procedure described in Install the V4L2Loopback Driver on a Linux Machine.

4. Navigate to the tarball folder and run the `install_viewagent.sh` script as a superuser. Include the command-line parameters for any optional features that you want to install.

For more information, see Command-line Options for Installing Horizon Agent for Linux .

For example, to install Horizon Agent with automatic acceptance of the VMware General Terms and with both the Real-Time Audio-Video feature and USB Redirection feature added:

```
sudo ./install_viewagent.sh -A yes -U yes -a yes --webcam
```

Note If you are installing Horizon Agent on a physical machine, you must include the `-M no` parameter to specify unmanaged mode as described in Prepare a Physical Linux Machine for Desktop Deployment.

5 Type **`Yes`** to accept the VMware General Terms if you run `install_viewagent.sh` without specifying the `-A` parameter.

The installer does not run unless you accept the VMware General Terms.

6 Allow the installation to proceed without interruption.

7 Restart the Linux machine for the changes to take effect.

8 Verify that the *viewagent* service is started by running the following command.

```
sudo service viewagent status
```

(RHEL 8.x) Install Horizon Agent Using the Digitally Signed RPM Installer

Note If you are installing Horizon Agent on a machine running a Linux distribution other than RHEL 8.x, do not use these instructions. Instead, use the procedure described earlier in this article.

1 Download the Horizon Agent for Linux installer package from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Navigate to the download page for the current release ofVMware Horizon and then to the download page for VMware Horizon for 64-bit Linux.

Download the Horizon Agent RPM package with filename `VMware-horizonagent-linux-`*`YYMM-y.y.y-xxxxxxx`*`.el8.x86_64.rpm`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxxx* is the build number.

2 Navigate to the folder of the downloaded RPM package and run the installer. For example:

```
sudo rpm -ivh VMware-horizonagent-linux-YYMM-y.y.y-xxxxxxx.el8.x86_64.rpm
```

3 Allow the installation to proceed without interruption.

Note The RPM package automatically installs Horizon Agent with the default feature options. After the installation, you can add features to the Horizon Agent configuration by running the `ViewSetup.sh` script.

4 Restart the Linux machine for the changes to take effect.

5. To support certain features, install the required drivers as follows.

   - To support the USB Redirection feature, install the VHCI driver as described in the "VHCI Driver for USB Redirection" section of System Requirements for Horizon Agent for Linux.
   - To support the Real-Time Audio-Video feature, complete the procedure described in Install the V4L2Loopback Driver on a Linux Machine.

6. To add more optional features to the Horizon Agent configuration or modify the configuration, run the `ViewSetup.sh` script as described in Command-line Options for Installing Horizon Agent for Linux .

   For example, to add both the Real-Time Audio-Video feature and USB Redirection feature:

   ```
   sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh -U yes -a yes --webcam
   ```

   Note If you are installing Horizon Agent on a physical machine, you must include the `–M no` parameter to specify unmanaged mode as described in Prepare a Physical Linux Machine for Desktop Deployment.

7. After installation, verify that the *viewagent* service is started by running the following command.

   ```
   sudo service viewagent status
   ```

Command-line Options for Installing Horizon Agent for Linux

This article describes the command-line parameters that you can use to install or bypass optional features for Horizon Agent on a Linux machine. You specify these parameters when running the Horizon Agent setup script in a terminal window.

Running the Horizon Agent for Linux Setup Script

In a terminal window, run the corresponding setup script for the installer format that you used to install Horizon Agent installer.

Horizon Agent Installer Format	Horizon Agent Setup Script
RPM (`.rpm`)	**Note** The RPM installer and setup script are supported only on RHEL 8.x machines. `sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh -optional parameter [parameter argument] . . .`
Tarball (`.tar.gz`)	`sudo ./install_viewagent.sh -optional parameter [parameter argument] . . .`

Command-line Options for Horizon Agent for Linux Setup Scripts

Unless otherwise noted, both the `install_viewagent.sh` and `ViewSetup.sh` scripts include the following optional parameters.

Table 3-21. Horizon Agent Optional Parameters

Optional Parameters	Description
--force	Force the installation of Horizon Agent on a Linux operating system that lies outside the scope of supported operating systems described in System Requirements for Horizon Agent for Linux. By default, this parameter is not included. **Note** This parameter is available for the `install_viewagent.sh` script only. Horizon feature support might be limited when running Horizon Agent on an unsupported operating system.
--help -h	Display help information and complete parameters list for the script.
--ipv6	Enable support for running Linux desktops and applications in an IPv6 environment. By default, this parameter is not included, meaning that IPv4 support is enabled.

--multiple-session	Enable support for multi-session published desktop pools and application pools based on a farm that includes the Linux virtual machine. By default, this parameter is not included.
	- To prepare the machine for use in an automated instant-clone farm, include the `--multiple-session` parameter in the installation script. For example:
	`sudo ./install_viewagent.sh --multiple-session`
	`sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh --multiple-session`
	- To prepare the machine for use in a manual farm, include both the **`--multiple-session`** parameter and the managed agent **`-M`** parameter set to **`no`**. For example:
	`sudo ./install_viewagent.sh --multiple-session -M no`
	`sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh --multiple-session  -M no`

--no-hosted-app	Deactivates support for single-session application pools running on desktops based on the Linux virtual machine. By default, this parameter is not included and support for single-session application pools is activated.
--no-vmwgreeter	Enables use of the Gnome Shell greeter in cases where Horizon 8 single sign-on (SSO) is deactivated or SSO credentials fail. By default, this parameter is not included and Horizon Agent uses the VMware greeter in cases where Horizon 8 SSO is deactivated or SSO credentials fail.
--webcam	Enables webcam redirection. By default, this parameter is not included. For more information, see Install Real-Time Audio-Video on a Linux Machine. **Note** To install the Real-Time Audio-Video feature, you must include both the webcam redirection (`--webcam)` and audio-in (`-a yes`) parameters. Webcam redirection is not supported in multiple-session mode, that is, when the `--multiple-session` parameter is included.
-a yes|no	Install or bypass support for audio input (audio-in) redirection. Default is **`no`**. **Note** To install the Real-Time Audio-Video feature, you must include both the audio-in (`-a yes`) and webcam redirection (`--webcam)` parameters.
-b	Hostname or IP address of the Horizon Connection Server. This parameter is only supported when you install Horizon Agent in unmanaged mode.
-d	Domain name of the Horizon Connection Server administrator. This parameter is only supported when you install Horizon Agent in unmanaged mode.

Table 3-21. Horizon Agent Optional Parameters (continued)

Optional Parameters	Description
-f yes|no	Install or bypass support of the cryptographic modules designed for Federal Information Processing Standards (FIPS) 140-2. Default is **no**. This option is supported only on RHEL 8.x machines. **Note** To support FIPS 140-2 mode, you must use Transport Layer Security (TLS) protocol version 1.2. You must also enable FIPS mode at the Linux system level and install a CA-signed certificate for the VMwareBlastServer daemon, as described in Configure a FIPS-compliant Linux Machine.
-j	JMS SSL keystore password. By default, installer generates a random string.
-k	Active Directory address of the Horizon Connection Server administrator. This parameter is only required for Kerberos authentication and is only supported when you install Horizon Agent in unmanaged mode.
-m yes|no	Install or bypass the smart card redirection feature. Default is **no**.
-n	Name of the Linux machine. This parameter is only supported when you install Horizon Agent in unmanaged mode. Default is **hostname**.
-p	Administrator password for the Horizon Connection Server. This parameter is only supported when you install Horizon Agent in unmanaged mode.
-r yes|no	Restart the system automatically after installation. Default is **no**.
-s	Common Name (CN) of the self-signed certificate for VMwareBlastServer. Default is **Blast**. This parameter is only supported when you install Horizon Agent in unmanaged mode
-u	User name of the Horizon Connection Server administrator. This parameter is only supported when you install Horizon Agent in unmanaged mode.
-A yes |no	For `install_viewagent.sh`, automatically accept or refuse the VMware General Terms and Federal Information Processing Standards (FIPS) statement. You must specify **yes** to proceed with the installation. If you do not specify this parameter in the `install_viewagent.sh` script, you must manually accept the VMware General Terms and FIPS statement during the installation.
-B	Domain name of the Horizon Connection Server host. This parameter is only required for Kerberos authentication when the Horizon Connection Server host and administrator have different domains. This parameter is only supported when you install Horizon Agent in unmanaged mode.
-C yes|no	Install or bypass the Clipboard Redirection feature. Default is **yes**.
-F yes|no	Install or bypass the Client Drive Redirection (CDR) feature. Default is **yes**.
-K	Active Directory address of the Horizon Connection Server host. This parameter is only required for Kerberos authentication when the Horizon Connection Server host and administrator have different domains. This parameter is only supported when you install Horizon Agent in unmanaged mode.
-M yes|no	Install Horizon Agent in managed or unmanaged mode. Default is **yes**. When you install Horizon Agent in managed mode, the Linux machine is managed by the vCenter Server instance associated with the Horizon Connection Server. When you install Horizon Agent in unmanaged mode, the Linux machine is not managed by the vCenter Server instance associated with the Horizon Connection Server.
-P yes|no	Install or bypass VMware Integrated Printing, which supports client printer redirection. Default is **yes**.

Table 3-21. Horizon Agent Optional Parameters (continued)

Optional Parameters	Description
-R	Register the Linux machine with the Horizon Connection Server host. Use this parameter to perform a new registration or to re-register a machine after changing between managed and unmanaged modes.
-S yes|no	Install or bypass support for single sign-on (SSO). Default is **`yes`**.
-T yes|no	Install or bypass the True Single Sign-on (True SSO) feature. Default is **`no`**.
-U yes|no	Install or bypass the USB Redirection feature. Default is **`no`**.

Table 3-22. Examples of Horizon Agent Setup Scripts with Parameters

Scenario	Example Script
Perform fresh installation and automatically accept the VMware General Terms and FIPS statement	`sudo ./install_viewagent.sh -A yes`

Enable smart card redirection	`sudo ./install_viewagent.sh -A yes -m yes`
	`sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh -m yes`

Bypass SSO support	`sudo ./install_viewagent.sh -S no`
	`sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh -S no`

Enable support for published desktop pools and application pools based on an automated instant-clone farm	`sudo ./install_viewagent.sh --multiple-session`
	`sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh --multiple-session`

Enable support for published desktop pools and application pools based on a manual farm	`sudo ./install_viewagent.sh --multiple-session -M no`
	`sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh --multiple-session -M no`

Install Real-Time Audio-Video on a Linux Machine

To install the Real-Time Audio-Video feature on a Linux machine, you must install both the V4L2Loopback driver and Horizon Agent with the audio-in and webcam redirection options included. You must include both options to complete the installation of Real-Time Audio-Video.

For information about how the Real-Time Audio-Video feature works and about feature limitations, see the sections at the end of this article. Also, see the topics under "Configuring Real-Time Audio-Video" in the *Horizon Remote Desktop Features and GPOs* document.

System Requirements for Real-Time Audio-Video

To support Real-Time Audio-Video, your deployment must meet certain software and hardware requirements.

Virtual desktops

The Linux desktop must be running one of the following distributions.

- Ubuntu 22.04/20.04
- Debian 12.x/11.x/10.x
- RHEL 9.x/8.x/7.x

  Note For RHEL 9.x desktops, ensure that you have enabled audio input and output redirection by installing the PulseAudio sound server. For more information, see Features of Linux Desktops in VMware Horizon 8.

- Rocky Linux 9.x/8.x
- SLED/SLES 15.x

When using Microsoft Teams with Real-Time Audio-Video, desktops must have a minimum of 4 vCPUs and 4 GB of RAM.

Horizon Client software

Horizon Client for Windows, Linux, Mac, iOS, or Android.

Horizon Client computer or client access device

- All operating systems that run Horizon Client for Windows, Mac, iOS, and Android.
- All operating systems that run Horizon Client for Linux on x64 devices. This feature is also supported on Raspberry Pi 4 Model B devices running ThinLinX Operating System (TLXOS) or Stratodesk NoTouch Operating System.
- For information about supported client operating systems, see the Horizon Client installation and setup document for the appropriate system or device.
- The webcam and audio device drivers must be installed, and the webcam and audio device must be operable, on the client computer. You do not need to install the device drivers on the machine where the agent is installed.

Installation Sequence for Real-Time Audio-Video

The Real-Time Audio-Video feature has a dependency on the V4L2Loopback driver. To support the feature, you must install both Horizon Agent and the V4L2Loopback driver on the Linux machine, in the correct sequence for your Horizon Agent installer.

Use the following guidelines to determine the appropriate installation sequence for the Real-Time Audio-Video feature.

Installation Sequence When Using the Tarball Horizon Agent Installer

If you want to install Horizon Agent using the `.tar.gz` tarball installer, follow this installation sequence.

1 Install the V4L2Loopback Driver on a Linux Machine.

2 Install Horizon Agent with both the audio-in and webcam redirection options.

```
sudo ./viewagent_installer.sh -a yes --webcam
```

For more information, see Install Horizon Agent on a Linux Machine.

Installation Sequence When Using the RPM Horizon Agent Installer

If you want to install Horizon Agent using the `.rpm` RPM installer, follow this installation sequence.

1 Install Horizon Agent, as described in Install Horizon Agent on a Linux Machine.

2 Install the V4L2Loopback Driver on a Linux Machine.

3 Use the Horizon Agent setup script to enable both the audio-in and webcam redirection options.

```
sudo /usr/lib/vmware/viewagent/bin/viewSetup.sh -a yes --webcam
```

See Command-line Options for Installing Horizon Agent for Linux .

Configuration Settings for Real-Time Audio-Video

You can use options in the `/etc/vmware/config` configuration file to define certain settings for the Real-Time Audio-Video feature, such as the maximum frame rate and image resolution allowed. See Edit Configuration Files on a Linux Desktop.

In addition, client users can configure a preferred device that Real-Time Audio-Video redirects to the remote desktop or published application. See "Selecting Preferred Webcams and Microphones" and "Selecting a Preferred Speaker" in the *Horizon Remote Desktop Features and GPOs* document.

How Real-Time Audio-Video Works

Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications, and supports standard webcams, audio USB devices, and analog audio input. This feature redirects video and audio data with a significantly lower bandwidth than can be achieved by using USB redirection.

Real-Time Audio-Video allows users to run Skype, Webex, Google Hangouts, Microsoft Teams, and other online conferencing applications in their remote sessions. With Real-Time Audio-Video, webcam and audio devices connected locally to the client system are redirected to the remote sessions.

During the setup of a conferencing application, users can choose input and output devices from menus in the application.

Note If end users change the resolution or frame rate (fps) setting on the client system, they must disconnect and reconnect to the Linux desktop session, and close and reopen all conferencing and video applications, to apply the changes to Real-Time Audio-Video redirection.

For Linux remote desktop and application sessions, Real-Time Audio-Video can redirect only one audio device and only one video device. The name of the audio device appears as **PulseAudio server (local)** and the name of the video device appears as **VMware Virtual Webcam**.

The VMware Virtual Webcam uses a kernel-mode webcam driver that provides enhanced compatibility with browser-based video applications and other third-party conferencing software.

When a conferencing or video application is launched, it displays and uses these VMware virtual devices, which handle the audio-video redirection from the locally-connected devices on the client.

Limitations of Real-Time Audio-Video

The Real-Time Audio-Video feature has the following limitations for Linux remote desktop and application sessions.

- The feature is not supported in multiple-session mode.
- The feature can redirect only one audio device and only one video device per session.

Install the V4L2Loopback Driver on a Linux Machine

To support the Real-Time Audio-Video feature on a Linux machine, you must install the V4L2Loopback driver. The Real-Time Audio-Video feature redirects locally connected webcam and audio devices from the client system to the remote session.

You must install version v0.12.5 of the V4L2Loopback driver on the Linux machine either before or after installing Horizon Agent, depending on the format of the Horizon Agent installer that you use. For more information, see Install Real-Time Audio-Video on a Linux Machine.

First, download version v0.12.5 of the V4L2Loopback source code package from https://github.com/umlaeute/v4l2loopback/tags. Then follow the installation procedure for your Linux distribution.

Install V4L2Loopback on an Ubuntu/Debian Machine

1 Install the required dependency packages.

```
sudo apt-get install make
sudo apt-get install gcc
sudo apt-get install libelf-dev
```

2 Compile and install the V4L2Loopback driver from the source code package.

```
unzip v0.12.5.zip
cd v4l2loopback-0.12.5

# For tarball installer, the [agent patch path] is the installer package path such as /
root/VMware-horizonagent-linux-x86_64-2206-8.6.0-19639256
# For RPM installer, the [agent patch path] is /usr/lib/vmware/viewagent
patch -p1 < [agent patch path]/resources/v4l2loopback/v4l2loopback.patch
make clean && make && make install

# Install v4l2loopback-ctl
make install-utils
depmod -A
```

3 (Only for Linux kernel version 5.15.0 and later) Modify the configuration to override the invalid V4L2Loopback driver installed by default on the machine with the valid V4L2Loopback driver that you just installed.

a Append the following line to the end of the `/etc/depmod.d/ubuntu.conf` configuration file.

```
override v4l2loopback * extra
```

b Regenerate the `modules.dep` file.

```
depmod -a
```

c To remove the invalid V4L2Loopback driver, do one of the following.

- Restart the machine.
- Run the following command.

```
sudo rmmod v4l2loopback
```

4 (Ubuntu only) If you have enabled the Extensible Firmware Interface (EFI) and UEFI Secure Boot on the Ubuntu virtual machine, configure signing settings for the V4L2Loopback driver.

a Create an SSL key pair for the V4L2Loopback driver.

```
openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER
-out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/" -addext
extendedKeyUsage=1.3.6.1.5.5.7.3.3
```

b Sign the V4L2Loopback driver.

```
sudo /usr/src/linux-headers-$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./
MOK.der  /lib/modules/$(uname -r)/extra/v4l2loopback.ko
```

c Register the key for UEFI Secure Boot.

```
sudo mokutil --import MOK.der
```

Note This command issues a request to set a Machine Owner Key (MOK) password for UEFI Secure Boot.

d To set up UEFI Secure Boot in the vSphere console, reboot the system. For more information, see https://sourceware.org/systemtap/wiki/SecureBoot.

Install V4L2Loopback on a RHEL or Rocky Linux Machine

1 Install the required dependency packages.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
sudo yum install patch
sudo yum install elfutils-libelf-devel
```

2 Compile and install the V4L2Loopback driver from the source code package.

```

unzip v0.12.5.zip
cd v4l2loopback-0.12.5

# For tarball installer, the [agent patch path] is the installer package such as /root/
VMware-horizonagent-linux-x86_64-2206-8.6.0-19639256
# For RPM installer, the [agent patch path] is /usr/lib/vmware/viewagent
patch -p1 < [agent patch path]/resources/v4l2loopback/v4l2loopback.patch
make clean && make && make install

# Install v4l2loopback-ctl
make install-utils
depmod -A
```

3 (RHEL and Rocky Linux 9.x/8.x) Configure signing settings for the V4L2Loopback driver.

   a Create an SSL key pair for the V4L2Loopback driver.

   ```
   openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER
   -out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/" -addext
   extendedKeyUsage=1.3.6.1.5.5.7.3.3
   ```

   b Sign the V4L2Loopback driver.

   ```
   sudo /usr/src/kernels/$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/
   modules/$(uname -r)/extra/v4l2loopback.ko
   ```

   c Register the key for UEFI Secure Boot.

   ```
   sudo mokutil --import MOK.der
   ```

   Note This command issues a request to set a Machine Owner Key (MOK) password for UEFI Secure Boot.

   d To set up UEFI Secure Boot in the vSphere console, reboot the system. For more information, see https://sourceware.org/systemtap/wiki/SecureBoot.

Install V4L2Loopback on a SLED/SLES Machine

1 Find the version of the current kernel package.

```
rpm -qa | grep kernel-default-$(echo $(uname -r) | cut -d '-' -f 1,2)
```

The output is the name of the kernel package currently installed. If, for example, the package name is `kernel-default-4.4.21-90.1`, then the current kernel package version is 4.4.21-90.1.

2 Install the `kernel-devel`, `kernel-default-devel`, `kernel-macros`, and the `patch` packages. For example, if the kernel package version is 4.4.21-90.1, use the following command.

```
zypper install --oldpackage kernel-devel-4.4.21-90.1 kernel-default-devel-4.4.21-90.1
kernel-macros-4.4.21-90.1 patch
```

3 Compile and install the V4L2Loopback driver from the source code package.

```

unzip v0.12.5.zip
cd v4l2loopback-0.12.5

# For tarball installer, the [agent patch path] is the installer package such as /root/
VMware-horizonagent-linux-x86_64-2206-8.6.0-19639256
# For RPM installer, the [agent patch path] is /usr/lib/vmware/viewagent
patch -p1 < [agent patch path]/resources/v4l2loopback/v4l2loopback.patch
make clean && make && make install
```

```
# Install v4l2loopback-ctl
make install-utils
depmod -A
```

4 Configure signing settings for the V4L2Loopback driver.

a Create an SSL key pair for the V4L2Loopback driver.

```
openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER
-out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/" -addext
extendedKeyUsage=1.3.6.1.5.5.7.3.3
```

b Find the path to the signing file for the V4L2Loopback driver.

```
sudo find / -name sign-file
```

This command returns the paths to all the signing files located on the system. The signing file path for the V4L2Loopback driver resembles the following example.

```
/usr/src/linux-5.3.18-24.9-obj/x86_64/default/scripts/
```

c Sign the V4L2Loopback driver. In the following command sequence, *<sign-file-path>* is the path to the signing file that you found earlier.

```
sudo /<sign-file-path>/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/$(uname -r)/
extra/v4l2loopback.ko
```

d Register the key for UEFI Secure Boot.

```
sudo mokutil --import MOK.der
```

Note This command issues a request to set a Machine Owner Key (MOK) password for UEFI Secure Boot.

e To set up UEFI Secure Boot in the vSphere console, reboot the system. For more information, see https://sourceware.org/systemtap/wiki/SecureBoot.

Install a CA-signed Certificate for VMwareBlastServer on a Linux Machine

By default, the Horizon Agent for Linux installer generates a self-signed certificate for the VMwareBlastServer daemon, which handles communications with clients using the Blast display protocol. To comply with industry or security regulations, you can replace the self-signed certificate for VMwareBlastServer with a certificate that is signed by a Certificate Authority (CA).

- When the Blast Security Gateway is not enabled on the Horizon Connection Server, VMwareBlastServer presents the default self-signed certificate to the browser that uses HTML Access to connect to the Linux desktop.
- When the Blast Security Gateway is enabled on the Horizon Connection Server, the Blast Security Gateway presents its certificate to the browser.

To replace the default self-signed certificate for VMwareBlastServer with a CA-signed certificate, you can use one of the following methods.

- **BCFKS keystore**: With this method, you use the `DeployBlastCert.sh` deployment script to store the certificate and private key in an encrypted Bouncy Castle FIPS keystore (BCFKS) in the `/etc/vmware/ssl` directory.
- **Unencrypted storage**: With this method, you manually copy the certificate and private key, without encryption, to the root level of the `/etc/vmware/ssl` directory.

The VMwareBlastServer daemon first looks in the Linux keyring for the certificate and private key from a BCFKS keystore. If it does not find a BCFKS keystore, it then reads the certificate and private key stored at the root level of `/etc/vmware/ssl`.

Deploy the VMwareBlastServer CA Certificate to a BCFKS Keystore

The `DeployBlastCert.sh` deployment script creates a new BCFKS keystore named `vmwareblast.bcfks` in the `/etc/vmware/ssl` directory and stores the certificate and private key in this keystore. The information in the keystore is then added to the Linux keyring.

1. Use the **SSLCertName** and **SSLKeyName** configuration options to customize the certificate name and private key name, respectively, as they will appear in the Linux keyring. For more information, see Table 6-2. Configuration Options in /etc/vmware/viewagent-custom.conf.
2. Run the `DeployBlastCert.sh` deployment script, as shown in the following example.

   ```
   sudo /usr/lib/vmware/viewagent/bin/DeployBlastCert.sh -c /root/rui.cert -k /root/rui.key
   ```

   Use the following parameter flags for the deployment script:

Parameter Flag	Description
-c	Specifies the CA-signed certificate file.
-k	Specifies the private key file.

Deploy the VMwareBlastServer CA Certificate to Unencrypted Storage

1. Add the private key and the CA-signed certificate to `/etc/vmware/ssl`.
   a. Rename the private key to **rui.key** and the certificate to **rui.crt**.
   b. Set read and executable permissions on `/etc/vmware/ssl`.

      ```
      sudo chmod 550 /etc/vmware/ssl
      ```

   c. Copy **rui.key** and **rui.crt** to `/etc/vmware/ssl`.
   d. Remove executable permissions on `/etc/vmware/ssl`.

      ```
      sudo chmod 440 /etc/vmware/ssl
      ```

2. Install the root and intermediate CA certificates into the Linux OS Certificate Authority store.

For information about other system settings that must be changed to support the CA certificate chain, refer to the documentation for your Linux distribution.

Configure a FIPS-compliant Linux Machine

To configure a Linux virtual machine that meets the requirements of the Federal Information Processing Standard (FIPS) 140-2 mode, follow the procedure described on this page. You must install Horizon Agent with FIPS mode enabled and then install a CA-signed certificate for the VMwareBlastServer daemon.

Prerequisites

Verify that you have completed the following prerequisites:

- Set up the virtual machine with vSphere Virtual Machine Encryption, recommended for increased security and protection. See Virtual Machine Encryption.
- Installed RHEL 8.x on the machine. FIPS 140-2 mode is only supported on machines running RHEL 8.x.
- Performed the relevant preparation steps described under Prepare a Linux Machine for Remote Desktop Deployment.

Procedure

1 On the RHEL 8.x machine, enable FIPS mode at the Linux system level.

```
sudo fips-mode-setup --enable
sudo reboot
```

2 Install Horizon Agent using the RPM installer.

For example:

```
sudo rpm -ivh VMware-horizonagent-linux-YYMM-y.y.y-xxxxxxx.el8.x86_64.rpm
```

For detailed instructions, see Install Horizon Agent on a Linux Machine.

3 Enable FIPS mode at the Horizon Agent level.

```
sudo /usr/lib/vmware/viewagent/bin/viewSetup.sh -f yes
```

For more information, see Command-line Options for Installing Horizon Agent for Linux .

4 Complete the steps described in Install a CA-signed Certificate for VMwareBlastServer on a Linux Machine.

5 Restart the machine.

```
sudo reboot
```

Results

You can now use the Linux machine to create desktop or application pools that are FIPS-compliant.

Upgrade Horizon Agent on a Linux Machine

You can upgrade Horizon Agent on a Linux machine by installing the latest version of Horizon Agent.

Prerequisites

- Verify that the `VMwareBlastServer` process is not running. To stop this process, use one of the following methods:
  - Ensure that the user logs out of the machine and no desktop session is active.
  - Restart the virtual machine.
- If you plan to upgrade Horizon Agent using the tarball installer, review the optional parameters for the `install_viewagent.sh` setup script. See Command-line Options for Installing Horizon Agent for Linux .
- If you plan to upgrade Horizon Agent on a virtual machine, open a Terminal window. You can run the Horizon Agent installation commands from the Terminal.
- If you plan to upgrade Horizon Agent on a physical host machine, open a Secure Shell (SSH) connection to the machine. SSH is the recommended method for running Horizon Agent installation commands on a physical machine. In addition, stop the X server and Gnome Display Manager as described in Prepare a Physical Linux Machine for Desktop Deployment.

Horizon Agent for Linux Upgrade Process

Note For general guidelines on upgrading desktop pools, see "Upgrading Published and Virtual Desktops" in the *Horizon 8 Installation and Upgrade* document, which is available in the VMware Horizon Documentation portal.

When upgrading Horizon Agent on RHEL 8.x, you can choose between the following installer formats:

- The `.tar.gz` installer package, which is not digitally signed. The existing Horizon Agent feature configuration and virtual machine deployment mode are not automatically preserved. To keep the existing configuration, you must include the appropriate feature parameters when running the installer.
- The `.rpm` installer package, which is digitally signed. The existing Horizon Agent feature configuration and virtual machine deployment mode are automatically preserved.

When upgrading Horizon Agent on a Linux distribution other than RHEL 8.x, you must use the `.tar.gz` installer package. To keep your existing feature configuration, you must include the appropriate feature parameters when running the installer.

In addition, you can choose between two types of virtual machine deployment, as described in the following sections.

Unmanaged Machine Deployment

- This type of upgrade is available for existing unmanaged virtual and physical machines. Unmanaged mode is a requirement for physical machines.
- The Horizon Agent installer registers the virtual machine to Horizon Connection Server which requires broker admin information.
- The Desktop Pool Creation wizard uses **Other Sources** in the Machine Source page to select the registered virtual machine.

Managed Virtual Machine Deployment

- This type of upgrade is available for unmanaged or managed virtual machines.
- The Horizon Agent installer does not communicate with Horizon Connection Server.
- The Desktop Pool Creation wizard uses **vCenter virtual machines** in the Machine Source page to select the virtual machines through vCenter.
- The deployment supports the following functions:
  - Remote Machine Power Policy
  - Allow users to reset their machines

You can use the following methods to upgrade an unmanaged virtual machine:

- Retain the unmanaged virtual machine deployment while upgrading to the latest version of Horizon Agent. This upgrade scenario does not require any configuration modifications in Horizon Connection Server.
- Upgrade from an unmanaged virtual machine deployment to a managed virtual machine deployment that uses the latest version of Horizon Agent. This upgrade scenario requires the creation of a new desktop pool based on the virtual machine.

Note To ensure the best possible performance, upgrade to a managed virtual machine deployment. The Horizon Agent upgrade does not support conversion of a managed virtual machine deployment to an unmanaged virtual machine deployment.

Upgrade Horizon Agent for Linux Using the Unsigned Tarball Installer

If you are upgrading Horizon Agent on a physical machine, review the information in Prepare a Physical Linux Machine for Desktop Deployment for additional steps and prerequisites.

Note For a RHEL 8.x machine, you also have the option to install Horizon Agent using a digitally signed installer. See the procedure described later in this article.

1 (RHEL 8.x) If your existing Horizon Agent version was installed using a digitally signed RPM installer, uninstall the agent software as described in Uninstall Horizon Agent From a Linux Machine.

2 Download the latest tarball installer for Horizon Agent for Linux from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   a Navigate to the download page for the current release of VMware Horizon and then to the download page for VMware Horizon for 64-bit Linux.

   b Download the Horizon Agent installer tarball with filename `VMware-horizonagent-linux-x86_64-YYMM-y.y.y-xxxxxxx.tar.gz`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxxx* is the build number.

3 Unpack the tarball for your Linux distribution. For example:

```
tar -xzvf VMware-horizonagent-linux-x86_64-YYMM-y.y.y-xxxxxxx.tar.gz
```

4 To support certain features, install the required drivers as follows.

   - To support the USB Redirection feature, install the VHCI driver as described in the "VHCI Driver for USB Redirection" section of System Requirements for Horizon Agent for Linux.
   - To support the Real-Time Audio-Video feature, complete the procedure described in Install the V4L2Loopback Driver on a Linux Machine.

5 Navigate to the tarball folder and run the `install_viewagent.sh` script according to one of the following upgrade scenarios. Also, include the command-line parameters for any optional features that you want to install, such as USB Redirection.

   For a detailed list of the optional parameters available for the `install_viewagent.sh` script, see Command-line Options for Installing Horizon Agent for Linux .

Scenario	Script Command
Upgrade an unmanaged virtual machine deployment and retain the unmanaged virtual machine deployment	`sudo ./install_viewagent.sh -A yes -M no` This upgrade scenario does not require the creation of a new desktop pool. You can reuse the existing desktop pool based on the virtual machine. **Note** To ensure the best possible performance, refrain from deploying an unmanaged virtual machine and deploy a managed virtual machine instead.
Upgrade an unmanaged virtual machine deployment and change it to managed virtual machine deployment	`sudo ./install_viewagent.sh -A yes -M yes` **Note** In Horizon Agent, delete the existing desktop pool from the unmanaged virtual machine deployment and create a new desktop pool for the managed virtual machine deployment. For more info, see Create a Manual Desktop Pool.
Upgrade a managed virtual machine deployment	`sudo ./install_viewagent.sh -A yes -M yes` **Note** After upgrading Horizon Agent, you can reuse the existing desktop pool based on the virtual machines.

6 Restart the Linux machine for the changes to take effect.

(RHEL 8.x) Upgrade Horizon Agent for Linux Using the Digitally Signed RPM Installer

If you are upgrading Horizon Agent on a physical machine, review the information in Prepare a Physical Linux Machine for Desktop Deployment for additional steps and prerequisites.

Note If you are upgrading Horizon Agent on a machine running a Linux distribution other than RHEL 8.x, do not use these instructions. Instead, use the procedure described earlier in this article.

1. If your existing Horizon Agent version was installed using an unsigned tarball installer, uninstall the agent software as described in Uninstall Horizon Agent From a Linux Machine.
2. Download the Horizon Agent for Linux RPM installer from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   a. Navigate to the download page for the current release ofVMware Horizon and then to the download page for VMware Horizon for 64-bit Linux.

   b. Download the Horizon Agent RPM package with filename `VMware-horizonagent-linux-YYMM-y.y.y-xxxxxxx.el8.x86_64.rpm`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxxx* is the build number.
3. Navigate to the folder of the downloaded RPM package and run the installer in upgrade mode. For example:

   ```
   sudo rpm -Uvh VMware-horizonagent-linux-YYMM-y.y.y-xxxxxxx.el8.x86_64.rpm
   ```

   Allow the upgrade to proceed without interruption. The RPM package upgrades Horizon Agent to the current version and preserves the existing Horizon Agent configuration.
4. Restart the Linux machine for the changes to take effect.
5. To support certain features, install the required drivers as follows.

   - To support the USB Redirection feature, install the VHCI driver as described in the "VHCI Driver for USB Redirection" section of System Requirements for Horizon Agent for Linux.
   - To support the Real-Time Audio-Video feature, complete the procedure described in Install the V4L2Loopback Driver on a Linux Machine.
6. To add more optional features to the Horizon Agent configuration or modify the configuration, run the `ViewSetup.sh` script as described in Command-line Options for Installing Horizon Agent for Linux .

   For example, to add both the Real-Time Audio-Video feature and USB Redirection feature:

   ```
   sudo /usr/lib/vmware/viewagent/bin/viewSetup.sh -U yes -a yes --webcam
   ```

Uninstall Horizon Agent From a Linux Machine

To uninstall Horizon Agent from a Linux machine, you must uninstall the Horizon Agent service and software and remove certain configuration files.

Prerequisites

- Verify that the `VMwareBlastServer` process is not running. To stop this process, use one of the following methods:
  - Ensure that the user logs out from the machine and no desktop session is active.
  - Restart the machine.
- If you plan to remove Horizon Agent from a virtual machine, open a Terminal window. You can run the Horizon Agent uninstallation commands from the Terminal.
- If you plan to remove Horizon Agent from a physical host machine, open a Secure Shell (SSH) connection to the machine. SSH is the recommended method for running Horizon Agent uninstallation commands on a physical machine.

Procedure

1 Run the appropriate uninstallation command for your Horizon Agent installer type.

Horizon Agent Installer Type	Horizon Agent Uninstallation Command
RPM (`.rpm`)	`sudo rpm -e VMware-horizonagent-linux-`*YYMM-y.y.y-xxxxxxx*`.el8.x86_64.rpm`
Tarball (`.tar.gz`)	`sudo /usr/lib/vmware/viewagent/bin/uninstall_viewagent.sh`

The command stops the Horizon Agent processes and deletes the Horizon Agent service and software from the `/usr/lib/vmware/viewagent` directory.

2 Manually delete the Horizon Agent configuration files from the `/etc/vmware` directory. For example:

```
sudo rm -rf /etc/vmware
```

Creating Virtual Machine Templates for Full-Clone Virtual Desktops

You must create a virtual machine template before you can create an automated pool that contains full-clone virtual machines.

A virtual machine template is a main copy of a virtual machine that can be used to create and provision new virtual machines. Typically, a template includes an installed guest operating system and a set of applications.

You create virtual machine templates in vSphere Client. You can create a virtual machine template from a previously configured virtual machine, or you can convert a previously configured virtual machine to a virtual machine template.

For information on using vSphere Client to create virtual machine templates, see the *vSphere Virtual Machine Administration* guide on the VMware vSphere Documentation portal. See Chapter 8 Create and Manage Automated Full-Clone Desktop Pools for information on creating automated pools.

Note A virtual machine template is not for creating an instant-clone desktop pool.

Configure a Virtual Machine with Multiple NICs for Horizon Agent

When you install Horizon Agent on a virtual machine that has more than one NIC, you must configure the subnet that Horizon Agent uses. The subnet determines which network address Horizon Agent provides to the Connection Server instance for client protocol connections.

Procedure for Windows Machines

On the virtual machine on which Horizon Agent is installed, open a command prompt, type *regedit.exe* and create a registry entry to configure the subnet.

For example, in an IPv4 network:

```
HKLM\Software\VMware, Inc.\VMware VDM\IpPrefix = n.n.n.n/m (REG_SZ)
```

In this example, *n.n.n.n* is the TCP/IP subnet and *m* is the number of bits in the subnet mask.

Procedure for Linux Machines

On the virtual machine where Horizon Agent is installed, edit the `/etc/vmware/viewagent-custom.conf` file to specify the subnet.

- In an IPv4 environment, configure the value for `Subnet` using CIDR notation, for example:

  ```
  Subnet=192.168.1.0/24
  ```

- In an IPv6 environment, configure the value for `Subnet6` using prefix/length notation, for example:

  ```
  Subnet6=2001:db8:abcd:0012::0/64
  ```

Using VMware Horizon Recording

The VMware Horizon Recording feature allows administrators to record desktop and application sessions to monitor user behavior for remote desktops and applications.

Administrators can observe a user's exact keystrokes, cursor and mouse activity, and other user behavior in a recorded desktop or application session. In addition to providing greater security and auditing for user behavior, recording also helps with troubleshooting and reproducing issues the user experiences during a session. Administrators can play back, store, and audit the recordings.

When a user logs on, Horizon Recording starts automatically, displaying the default message **Your session is being recorded in accordance with security policies**. The recording runs as long as the session is in a connected state. Recording stops when the user logs out or disconnects. If the user changes the screen resolution of the desktop or application session, Horizon Recording creates a new segment of the recording. Recording file sizes vary based on the duration of the connected session. Recordings are stored in MP4 format and can be downloaded to play in a local player or viewed in the Horizon Recording web console.

Components

Horizon Recording consists of the following components:

- **Horizon Recording Server**: Collects information about the session as well as raw recording data for storage and playback. This component is available for VMware Horizon 8 2106 and later.
- **Horizon Recording Agent**: Records a user session, registers the session with the Horizon Recording Server, and uploads recording data.
  - The Horizon Recording Agent for Windows is available for Horizon 8 2106 and later.
  - The Horizon Recording Agent for Linux is available for Horizon 8 2306 and later.

Installation files are available on VMware Customer Connect.

Note Like certain other Horizon 8 features, this feature is not available for every subscription. For more information, see VMware Horizon Subscription Feature comparison.

Web Interface

After you install the Horizon Recording Server (see the next section on this page), you can access the Horizon Recording web console at **https://<localservername>:9443**.

The web console displays the following:

- **Dashboard** includes a list of recent recordings, the server, database, and folder where recordings are stored, as well as recording information such as start time, duration, size, and state. You can lock, unlock, and delete recordings.
- **Recordings** includes a list of all recordings with information such as name, launched resource, location, start and end dates, start time, duration, size, and state. You can lock, unlock, and delete recordings.
- **Audit Trial** tracks all user actions in the user interface.

Install the Horizon Recording Server

Install the Horizon Recording Server component on a machine to collect information about the session as well as raw recording data for storage and playback.

The Horizon Recording Server component consists of these items:

- A database for session information storage and configuration
- A Windows NTFS folder for recording storage
- A web service for collecting recording data, administration, and playback

You can deploy the Horizon Recording Server as a standalone setup where the server is installed on a machine that leverages a local SQLite database stored in the installation directory as `local.db` and a local NTFS folder.

You can also deploy the Horizon Recording Server in a high availability environment using multiple servers behind a load balancer, leveraging Microsoft SQL or PostgreSQL databases, as well as a shared NTFS folder on all servers for storing recording data. Load balancers configured with L4 load distribution are supported.

Minimum Server Resource Requirements (required to support 2,000 active recordings)

Resource	Minimum Value
CPU	4 vCPU
Memory	8 GB
Free Disk Space	20 GB **Note** This depends on the type of applications the user runs in the session and also the frame change rate. You must monitor usage and add extra disk space as required.

Note The Horizon Recording Server is built in .Net Core and requires a 64-bit Windows Server operating system that is a member of the domain if you use group extraction. The server operating system must be Windows Server 2016 or later (64-bit).

To install the Horizon Recording Server, perform the following steps.

1. Download the `HorizonRecordingServer.exe` file and copy it to a local folder on the server.
2. Run the installer and follow the steps. Default credentials are shown below.

   Username/Password: **`administrator/Recording123`**

   The server is now available through the Horizon Recording web console: **https://<localservername>:9443**

3 Manually secure the recordings folder permissions so that only the recording server's active directory accounts have access to the folder to add, modify, or delete recordings.

- To uninstall the Horizon Recording Server, use Add Remove Programs (`appwiz.cpl`) to remove the Horizon Recording server binaries and then delete the following components manually:
  - The local database file (`local.db`) in `installation directory`
  - The logs located in `C:\programdata\VMware\Horizon Recording`
  - Local recordings located in `installation directory\Recordings`
- To reset the installation:

  a Stop the Horizon Recording service.

  b Delete the Recordings folder from the installation directory.

  c Delete the `servicesettings.json` file and the `local.db` file from the installation directory.

  d Start the Horizon Recording service.

  The `servicesettings.json` and `local.db` files are recreated afresh.

Install the Horizon Recording Server Using the Command Line

Administrators can perform a silent installation of the Horizon recording server as follows.

```
HorizonRecordingServer.exe /s /v/qn
```

Install the Horizon Recording Agent for Windows

Install the Horizon Recording Agent component on all Windows machines where you want to record sessions.

The Horizon Recording Agent registry settings are stored in `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Recording Agent`

Minimum Resource Requirements

Resource	Minimum Value (VDI)	Minimum Value (RDSH - 80 sessions)
CPU	2 vCPU	64 vCPU
Memory	2 GB	64 GB
Free Disk Space	5 GB **Note** This depends on the type of applications the user runs in the session and the frame change rate. You must monitor usage and add extra disk space as required.	50 GB **Note** This depends on the type of applications the user runs in the session and the frame change rate. You must monitor usage and add extra disk space as required.

Additional System Requirements

- Horizon 8 2106 or later for VDI; Horizon 8 2111 or later for RDSH
- Instant Clone Agent or Full Clone Agent
- **Note** Do not install the instant clone agent feature on the golden image (template) if you plan to deploy full clones.
- Windows 10 1909 or later 64-bit operating system for VDI; Windows Server 2016 or later 64-bit operating system for RDSH
- Microsoft .Net framework 4.6.1 or later
- VMware Blast
- Port 9443 allowed in the firewall inbound rules on the Horizon Recording Server

To install the Horizon Recording Agent for Windows, perform the following steps.

1 Download the `HorizonRecordingAgent.exe` file and copy it to a local folder.

2 Run the installer and follow the steps.

3 When prompted for the connection, provide the correct URL of the recording server in the format **`https://<FQDN or IP address of recording server>:9443`** along with the User Name and Password.

   a Select the **This machine is a template** check box if the machine is a parent VM and a pool will be created from it.

   b Click **Register**.

   c If the certificate of the server is untrusted, accept the thumbprint of the server when prompted.

- To uninstall the Horizon Recording Agent, use Add Remove Programs (`appwiz.cpl`) to remove the Horizon Recording agent binaries and then delete the following components manually:
  - Logs located in `C:\programdata\VMware\Horizon Recording`
  - Any local pending recordings located in `installation directory\Recordings`
- To delete the agents from the registered machines:

  a In **Administrator > Manage Agents**.

  b Select the Name of the agent and then click **Delete**.

  c Read the confirmation message carefully and proceed with the deletion.

Install the Horizon Recording Agent Using the Command Line

Administrators can perform a silent installation of the Horizon recording agent as follows.

```
HorizonRecordingAgent.exe /s /v/qn MACHINEISTEMPLATE="True/False"
SERVERADDRESSPROP="https://rec.server.fqdn:9443" USER_NAME="username"
USER_PASSWORD="Password" TRUSTEDTHUMBPRINT="thumbprint"
```

Command Line Option	Description
MACHINEISTEMPLATE	True (or) False
SERVERADDRESSPROP	FQDN (or) IP of Recording server (or) Load balancer. Note: Starts with `https://` and ends with port number 9443.
USER_NAME	Admin username of recording server.
USER_PASSWORD	Password of the Admin username.
TRUSTEDTHUMBPRINT	Thumbprint of the recording server (no spaces or no colons).

Requirements for the Horizon Recording Agent for Linux

Horizon Recording is supported on machines running the following Linux distributions:

- RHEL 8.x/9.x
- Rocky Linux 8.x/9.x
- RHEL/CentOS 7.9
- Ubuntu 20.04/22.04
- Debian 10.x/11.x/12.x
- SLED/SLES 15.x

Install the Horizon Recording Agent component on all Linux machines where you want to record sessions.

Note You must install Horizon Agent on the machine before installing the Horizon Recording Agent component.

Minimum Resource Requirements

Resource	Minimum Value (Single-session desktops/applications)	Minimum Value (Multi-session desktops/applications - 50 sessions)
CPU	2 vCPU	40 vCPU
Memory	2 GB	48 GB
Free Disk Space	5 GB **Note** This depends on the type of applications the user runs in the session and the frame change rate. You must monitor usage and add extra disk space as required.	50 GB **Note** This depends on the type of applications the user runs in the session and the frame change rate. You must monitor usage and add extra disk space as required.

Additional System Requirements

- Horizon 8 2306 or later
- Port 9443 allowed in the firewall inbound rules on the Horizon Recording Server

The installer for the Horizon Recording Agent for Linux is available in two different formats:

- Tarball installer
- RPM installer

Run the Linux Tarball Installer for Horizon Recording Agent

1. Install Horizon Agent on the Linux machine. See Install Horizon Agent on a Linux Machine.
2. Download the Horizon Recording Agent tarball package to a local directory on the agent machine.
3. Unpack the tarball.

   ```
   tar zxvf Horizon.Recording.Linux.Agent-x.x.x.x.tar.gz
   ```

4. Navigate to the tarball directory and run the appropriate installation command based on the type of resource pool that you plan to create from the agent machine.

Pool Type	Command
Instant-clone or full-clone pool (Append the `-t` parameter)	`sudo ./install.sh -u https://<Horizon Recording Server IP>:9443 -n <username> -p <password> -t`
Manual pool (Do not append the `-t` parameter)	`sudo ./install.sh -u https://<Horizon Recording Server IP>:9443 -n <username> -p <password>`

Note The `-t` parameter ensures that all clones created from the machine will have the Horizon Recording Agent installed and configured. For a description of all the required and optional parameters that you can include in the installation command, see Linux Installer Parameters for the Horizon Recording Agent.

Run the Linux RPM Installer for Horizon Recording Agent

1. Install Horizon Agent on the Linux machine. See Install Horizon Agent on a Linux Machine.
2. Download the Horizon Recording Agent RPM package to a local directory on the agent machine.
3. Run the command to install the RPM package.

   ```
   sudo rpm -ivh ./HorizonRecording.Linux.Agent-x.x.x.x.rpm
   ```

4 Locate `rpminstall.sh` in the `/usr/lib/vmware/horizonrecording/` directory. Continue the installation and configuration process by running the appropriate installation command based on the type of resource pool that you plan to create from the agent machine.

Pool Type	**Command**
Instant-clone or full-clone pool (Append the `-t` parameter)	`sudo /usr/lib/vmware/horizonrecording/rpminstall.sh -u https://<Horizon Recording Server IP>:9443 -n <username> -p <password> -t`
Manual pool (Do not append the `-t` parameter)	`sudo /usr/lib/vmware/horizonrecording/rpminstall.sh -u https://<Horizon Recording Server IP>:9443 -n <username> -p <password>`

Note The `-t` parameter ensures that all clones created from the machine will have the Horizon Recording Agent installed and configured. For a description of all the required and optional parameters that you can include in the installation command, see Linux Installer Parameters for the Horizon Recording Agent.

Linux Installer Parameters for the Horizon Recording Agent

These installer parameters apply to each of the following installer scripts:

- **install.sh** from the tarball package
- **rpminstall.sh** from the RPM package

Table 3-23. Required Parameters for the Horizon Recording Agent Installer Script

Required Parameter	**Description**
--uri -u	The session recording url, including `https://`.
--username -n	The user name for authenticating to the server.
--password -p	The password for authenticating to the server.

Table 3-24. Optional Parameters for the Horizon Recording Agent Installer Script

Optional Parameter	Description
--help -h	Display the help for using the installer script.

--trusted-ssl-certificate
-s
	The trusted SSL certificate thumbprint.
	Examples of supported formats:
	`59 2C E2 BD 6F 44 09 7F BF 8C 0F DA 66 6A 1C 3C 38 90 BE 24`
	`C8:E1:BD:B3:6F:22:E9:EA:60:35:19:D7:E0:F5:42:15:33:85:67:16`

--template -t	Ensures that all instant clones or full clones created from the machine will have the Horizon Recording Agent installed and configured.

Repair the Horizon Recording Agent Connection on Linux Machines

You can perform the steps described in this section if you face one of the following scenarios:

- The Horizon Recording Agent for Linux loses its trusted connection with the Horizon Recording Server.
- The Horizon Recording Agent for Linux requires registration with a new Horizon Recording Server.

The following procedure re-registers the trusted connection between the Horizon Recording Agent and the Horizon Recording Server.

1 On the agent machine, stop the horizonrecording.service daemon.

```
systemctl stop horizonrecording.service
```

2 Run the appropriate registration command based on the type of resource pool created from the agent machine.

Pool Type	Command

Instant-clone or full-clone pool
(Append the `-t` parameter)
	`sudo /usr/lib/vmware/horizonrecording/`
	`Horizon.Recording.xAgent.worker -register -url="https://`
	`<Horizon Recording Server IP>:9443"`
	`-username=<username> -password=<password> -thumbprint="<Horizon`
	`Recording Server Certificate Thumbprint>" -t`

Manual pool
(Do not append the `-t` parameter)
	`sudo /usr/lib/vmware/horizonrecording/`
	`Horizon.Recording.xAgent.worker -register -url="https://`
	`<Horizon Recording Server IP>:9443"`
	`-username=<username> -password=<password> -thumbprint="<Horizon`
	`Recording Server Certificate Thumbprint>"`

Note For a description of all the required and optional parameters that you can include in the registration command, see Linux Installer Parameters for the Horizon Recording Agent.

Horizon Recording Agent for Linux Logs

The Horizon Recording Agent for Linux saves activity logs to the `/var/log/vmware/horizonrecording` directory.

You can increase the logging detail by changing the minimum log level to "Trace".

Note Since the Horizon Recording Agent logs can increase rapidly in file size, it is recommended that you increase the logging detail only for troubleshooting purposes.

1 Modify the `/usr/lib/vmware/horizonrecording/Nlog.config` file as follows:

```
<logger name="*" minlevel="Trace" writeTo="ServiceLogging" />
```

2 To make the changes take effect, restart the horizonrecording.service daemon.

```
systemctl restart horizonrecording.service
```

Upgrade the Horizon Recording Server

Before upgrading the Horizon Recording Server, do the following:

- Confirm that there are no active recordings.
- Create a backup of the Recordings folder, the `servicesettings.json` file, and the `local.db` (if you are using SQLite for the database).

To upgrade the Horizon Recording Server, perform the following steps.

1 Download the `HorizonRecordingServer.exe` file.

2 Copy the `HorizonRecordingServer.exe` file to a local folder on the server.

3 Run `HorizonRecordingServer.exe`.

Note the following:

- By default, the server is upgraded in the same `C:\Program Files\VMware\Desktop Recording Server` folder.
  - If you change the upgrade location to a new folder, the configuration is not retained, and is treated as a fresh installation. As a result, you cannot access or play back the old recordings from the web console after the upgrade.
  - If you do not change the default location, then all the configurations are retained, and you can access and play back the recordings from the web console after the upgrade.
- After the upgrade, the log location for the server changes to a new `C:\ProgramData\VMware\Horizon Recording` folder. The old logs are still available in `C:\ProgramData\VMware\Horizon Desktop Recording`.

Upgrade the Horizon Recording Agent for Windows

Before upgrading the Horizon Recording Agent, confirm that there are no active recordings on the agent.

Note It is recommended to upgrade the server before upgrading the agent.

To upgrade the Horizon Recording Agent, perform the following steps.

1. Download the `HorizonRecordingAgent.exe` file.
2. Copy the `HorizonRecordingAgent.exe` file to a local folder on the agent.
3. Run `HorizonRecordingAgent.exe`.

Note the following:

- By default, the agent is upgraded in the same `C:\Program Files\VMware\Desktop Recording Agent` folder.

  If you change the upgrade location to a new folder, then the configuration is not retained, and is treated as a fresh installation.
- The Horizon Recording Server address is auto-populated during the upgrade procedure.
- After the agent is upgraded, the log location of the agent is changed to a new `C:\ProgramData\VMware\Horizon Recording` folder. The old logs are still available in `C:\ProgramData\VMware\Horizon Desktop Recording`.

Upgrade the Horizon Recording Agent for Linux

Before upgrading the Horizon Recording Agent, confirm that there are no active recordings on the agent.

Note It is recommended that you upgrade the server before upgrading the agent.

To upgrade the Horizon Recording Agent, follow the procedure for your installer type.

To upgrade Horizon Recording Agent using the tarball installer

1. Download and run the tarball installer for the new version of Horizon Recording Agent. For detailed instructions, see Run the Linux Tarball Installer for Horizon Recording Agent.
2. Restart the agent machine to apply the changes.

To upgrade Horizon Recording Agent using the RPM installer

1. Download the RPM installer package for the new version of Horizon Recording Agent and save the installer to a local directory on the agent machine.
2. Run the command to install the RPM package in upgrade mode.

   ```
   sudo rpm -Uvh HorizonRecording.Linux.Agent-x.x.x.x.rpm
   ```
3. Restart the agent machine to apply the changes.

Uninstall the Horizon Recording Agent for Linux

If you need to remove the Horizon Recording Agent from the agent machine, use the applicable uninstallation command.

- Tarball installer:

  ```
  sudo /usr/lib/vmware/horizonrecording/uninstall.sh
  ```

- RPM installer:

  ```
  sudo rpm -e HorizonRecording.Linux.Agent-x.x.x.x
  ```

Horizon Recording Settings

This topic describes settings for the VMware Horizon Recording feature.

Horizon Recording Settings in the Web Interface

In **Administrator > Manage Agents**, you can see the details of the machines that are registered with this instance of the recording server.

In **Administrator > Service Settings**, you can change the authentication, client, and server settings for the recording application, as well as recording criteria.

The following credentials are stored in the database. By default, the administrator has full control of the service settings, while the viewer can only find, watch, and download recordings.

Username/Password: **`administrator/Recording123`**

Username/Password: **`viewer/Recording456`**

You can select a user and change these passwords in **Authentication Settings**:

Authentication Settings	Description
LDAPS Integration	Disable or enable LDAPS integration. If enabled, enter the following information: ■ LDAPS URL ■ Bind User DN ■ Bind User Password ■ Search Base ■ Administrative Group DN ■ Viewer User Group DN ■ User Search Filter ■ Group Search Filter
Local Users	Select a user and click **Change Password** to change the password for that user.

Under **Client Settings**, the following settings affect the behavior of the Horizon Recording Agent:

Client Settings	Description
Notification Message	Message displayed to the user when their session is being recorded.
Split Recordings by Duration	Enable/Disable
Maximum Recording Duration	The maximum duration of a recording before it is stopped and a new recording is started (in minutes). Minimum value is 30; maximum value is 600. **Note** This setting appears only when the **Split Recordings by Duration** option is enabled.
Chunk size	The buffer size on the Horizon Recording Agent for each recording screen. When this buffer is filled, the data is submitted to the Horizon Recording Server.
Upload Interval	The length of time an active recording chunk will be uploaded to the server if the buffer has not yet filled. For example, if the interval is set to 5 minutes and the buffer has yet to fill, when this timespan has elapsed, the current recording screen data is uploaded to the server and a new chunk is created. This setting ensures a smaller window for missed recordings if the Horizon Recording Agent encounters a failure.

Under **Recording Criteria**, the following settings dictate the session types that are recorded:

Recording Criteria	Description
Record Local Sessions	Instructs the Horizon Recording Agent to record all sessions that are brokered from internal connection servers on the LAN.
Record Remote Sessions	Instructs Horizon Recording Agent to record all sessions that are brokered via a Unified Access Gateway.
Groups to record	Lists specific groups of users to be recorded using the session type recording criteria. If you do not add a group, all users will be evaluated for recording.

Under **Local Server Settings**, the following settings affect the local server currently connected to the database. To change local server settings, use the **Edit Deployment** wizard (see below).

Local Server Settings	Description
Database Connection Type	This local server setting is read from the `servicesettings.json` file on the local server. Supported database types are: ■ SQLite (local file) ■ MSSQL (Microsoft SQL) - Must be the same version of MSSQL database that is being used as the Connection Server Event database. ■ PostgreSQL - Must be the same version of PostgreSQL database that is being used as the Connection Server Event database.
Database Connection String	Identifies the server instance and database connection. Example: `Data Source=Local.db`

Under **Cluster Settings**, the following settings affect all the servers connected to the database. To change cluster storage location, use the **Edit Deployment** wizard (see below).

Cluster Settings	Description
Recording Storage Folder	File path of the folder in which the Horizon Recording Server stores active recording data or finished recordings. Location of this folder depends on the deployment type: NTFS Share or Local. This folder must be secured manually.
Encrypt Recordings	Enable/Disable **Note** Enabling this will encrypt the recordings before storing them on the file system. The recordings on the file system cannot be played because they are encrypted and in `.bin` format. Only the admin user that can log on to the web console should be able to view and play them, because they are not decrypted until the moment when playback is requested from the web console.
Conversion Chunk Size	Buffer size used to convert active recordings to finished recordings. The default value is 10.
Conversion Thread Count	The number of threads dedicated to converting finished raw recordings to MP4/binary format. Please do not change this value unless instructed to do so.
Conversion Wait Time	Amount of time a pending recording conversion has to wait before attempting to convert the files from active to finished. The default value is 10 minutes.
Raw Files	This setting affects both the Horizon Recording Agent and the Horizon Recording Server. ■ Horizon Recording Agent: instructs the agent to delete the recording when it has uploaded the data to the server successfully. ■ Horizon Recording Server: instructs the server to retain the raw files post conversion to MP4. This setting is enabled by default. Disabling this setting compromises the security of the files.
Retention Settings	Number of days a recording is retained on the server, after which the web service deletes the recordings. Locked recordings are excluded from the retention rules and remain on the server.

The SSL certificate used by the Horizon Recording Server is retrieved from the local machine's certificate store. It has a friendly name and a private key. If the SSL certificate does not exist, it is created on service startup. To install a custom certificate, rename the existing certificate to **`HorizonRecordingServer`** and install the certificate to the machine store. Restart the Horizon Recording Server service for the changes to take effect.

Note The SSL certificate must be trusted by the Horizon Recording Agent; otherwise the trusted thumbprints you added during installation will not contain the new certificate's thumbprint.

You can configure additional settings, such as the JWT token timeout and the SSL/TLS port, in the `servicesettings.json` file in the installation directory. You must stop the service before modifying this file and these settings only affect the server you modify. These settings must match on all recording servers participating in the cluster.

```
{
"HTTPSPort": 9443,
"DBConnectionString": "GlmrgliM0TpWt5nbC1RQyjoG]
"JWTTokenLifeSpan": 60,
"DBType": 1,
"ConnectionStringIsEncrypted": true
}
```

Edit Deployment Wizard

You can modify Horizon Recording Server settings with the **Edit Deployment** wizard.

Modifying Horizon Recording Server settings affect both the local server settings, such as the database connection, and the cluster's storage location. After the wizard completes, the local web service is restarted to update the database. Any changes to the storage location affect all servers in the cluster immediately.

Note Data is never migrated when modifying the deployment. Only the service configuration and user authentication details are migrated. Make sure to back up all recordings in the database by downloading the recordings, then deleting the sessions in advance to avoid having unwanted data.

Also note the following:

- In a standalone mode, you can only modify the local server’s database connection if there are no active sessions in progress.
- You can select the database type and connection string. These settings are encrypted and stored in the `servicesettings.json` file in the server installation directory. If the user specified in the connection string has permissions to create the database, the web service will create a database. Otherwise, pre-create an empty database with the desired name and verify that the account provided has the ability to create the required tables.
- The account must have the ability to make database layout changes for future upgrades where the database schema may change, and the web service will automatically perform the migrations.
- The web service will be restarted after the database has been instantiated and the local users and settings have been migrated.
- Modifying the cluster's storage location immediately affects all servers in the cluster. Do not modify the storage location when there are active recordings occurring. Data is not migrated when modifying the storage location.

Logging

By default, the Horizon Recording Server logs are located in `C:\programdata\VMware\Horizon Recording`.

For Windows desktops, the Horizon Recording Agent logs are located in `C:\programdata\VMware\Horizon Recording`.

For Linux desktops, the Horizon Recording Agent logs are located in `/var/log/vmware/horizonrecording`.

To troubleshoot any issues, you can extend the logging by modifying the `NLog.config file`. Changing the minlevel to Debug or Trace increases the size of the log files.

```
<rules>
/logger name="*" minlevel="Trace" writeTo="WebServiceLogging" />
</rules>
```

Horizon Recording Guidelines and Best Practices

This topic provides best practices for the VMware Horizon Recording feature.

Recording File Size Guidelines

Recording file size guidelines are as follows.

Screen Resolution	Recording Duration (HH:MM:SS)	Active Time (HH:MM:SS)	Size (with encryption enabled)	Size (with encryption disabled)	Reference Workload
640 x 480	01:00:46	00:52:18	40.90 MB	38.03 MB	LoginVSI Knowledge Worker Workload
1024 x 768	01:00:00	00:50:21	110.39 MB	112.19 MB	LoginVSI Knowledge Worker Workload
1920 x 1080	01:00:08	00:48:07	193.34 MB	188.94 MB	LoginVSI Knowledge Worker Workload
2366 x 1282	01:00:00	00:50:36	213.76 MB	207.87 MB	LoginVSI Knowledge Worker Workload
3840 x 2160	01:00:24	00:50:46	381.91 MB	353.72 MB	LoginVSI Knowledge Worker Workload

Recording Duration: The duration from user logon to user logoff.

Active Time: Amount of time the user interacted with the application or desktop. This is always less than or equal to the Recording Duration.

Reference Workload: LoginVSI Knowledge Worker workload running in the session to simulate the customer workload.

Note The data in this table is provided only as a guideline. The size will vary based on the application that is running, the frequency of keyboard strokes, mouse movements, screen resizing, frame change rate and so forth.

Installation and Configuration

- By default, the recording server installation points to a local SQLite DB which is suitable only for testing purposes. It is recommended to use MSSQL or PostgreSQL DB for production environments.
- It is recommended to use separate machines for Recording Server and Recording DB, preferably within the same datacenter and having less latency.

Agent Settings

- When Split Recording is enabled, the “Maximum Recording Duration” can be set to 60 minutes or more for better performance of the Recording Server.
- The “Chunk Size” can be set to 15 MB or more to avoid frequent uploads of the chunks to the recording server.
- The “Upload Interval” can be set to 15 minutes or more to avoid frequent uploads.

Using Horizon Recording with Load Balancer

For high availability, Horizon Recording can be installed on multiple servers and configured with a load balancer.

Here are the high-level steps to follow to use Horizon Recording with a load balancer. Details for each are provided in this topic.

1 Create a shared folder on a file server with appropriate permissions which is accessible from all the recording servers to be installed.

2 Install the Horizon Recording on multiple servers (preferably in the same datacenter). See "Install the Horizon Recording Server" in the Using VMware Horizon Recording topic for details.

3 Edit the deployment on all the recording servers to point to the same database and same shared folder. The database will store the recording metadata and the shared folder will store the actual recording files.

4 Configure L4 load balancing for Horizon recording servers on port 9443.

5 Install the Horizon Recording agent on the parent desktop by pointing to the load balancer's IP/FQDN while registering with the Horizon Recording server.

Edit the Deployment on the Recording Servers

For each recording server:

1 Navigate to **Administrator -> Service Settings -> Server Settings -> Edit Deployment**.

2 Read the message that displays and click Next.

3 If this is the first server you are editing, select **Configure Manually** and click Next. If this is not the first server to edit, skip to Step 4.

   a Select the required Database and copy the appropriate Connection String from the examples section and paste it into the Connection String box.

   b Modify the user id, password, server, database and Trusted_Connection with appropriate information and click Next.

   c In the storage location page, provide the shared folder which is accessible from all the recording servers. Click **Test Path** to verify if it is accessible, then click Next.

   d Click **Save Configuration**. If everything is fine the web service restarts and you are logged out.

   e Log in and verify that the configuration was saved properly.

4 For subsequent servers, select **Import configuration from an existing server**.

   a Enter the URL, username and password of the existing server and click **Import**. A message “Service settings imported successfully, please validate them on the following pages” displays if the credentials are valid.

   b Click Next and validate the configuration details in the “Database Type” page. They should match the configuration details in the existing server.

   c Click Next and validate the configuration details in the “Storage Location” page. They should match the configuration details in the existing server. You can test the path here as well.

   d Review the changes and click **Save Configuration**. If everything is fine, the web service restarts, and you are logged out.

   e Log in and verify that the configuration is saved properly.

Configure the L4 Load Balancer

The following are high level steps to configure a load balancer for recording servers. Note that the steps will change depending on which load balancer is used.

1 Create a virtual service with service port 9443 with SSL enabled. Then assign a virtual IP to the virtual service.

2 Create a pool of recording servers with port 9443.

3 Once the load balancer configuration is saved, access the web console using `https://<FQDN_or_IP_address_of_the_load_balancer>:9443`. If the load balancer configuration is correct, the UI will be accessible.

Install Horizon Recording Agent on the Parent Desktop

1. Download and run the Horizon Recording Agent installer, as described in Using VMware Horizon Recording.

   For Linux desktops, follow the instructions as documented, but modify the installation command as follows:

   - Tarball installer:

     ```
     sudo ./install.sh -u https://<FQDN or IP address of the load balancer>:9443 -n
     <username> -p <password> -t
     ```

   - RPM installer:

     ```
     sudo /usr/lib/vmware/horizonrecording/rpminstall.sh -u https://<FQDN or IP address of
     the load balancer>:9443 -n <username> -p <password> -t
     ```

2. When prompted for the connection, provide the correct URL of the load balancer in the format **`https://<FQDN or IP address of the load balancer>:9443`** along with the User Name and Password.

   a. Select the **This machine is a template** check box if the machine is a parent VM and a pool will be created from it.

   b. Click **Register**.

   c. If the certificate of the server is untrusted, accept the thumbprint of the server when prompted.

3. When recording agent installation is finished, log on to the recording server's web console using the load balancer IP and navigate to **Administrator -> Manage Agents**. The agent should be listed there with **Type** listed as **Template**.

   Note This can also be verified by logging into each recording server to make sure that the data is synced across all of the recording servers.

Setting Up Active Directory Integration and User Authentication Features for Linux Desktops

4

Horizon Agent uses the existing Microsoft Active Directory (AD) infrastructure for user authentication and management. You can integrate your Linux virtual machines with Active Directory so that users can log in to a Linux desktop using their Active Directory user account. You can also configure features for user authentication, such as single sign-on (SSO), smart card redirection, and True SSO.

Note Horizon Agent expects the Linux desktop and the client user to reside in the same Active Directory domain. If the desktop and user reside in different domains, Horizon Agent might misidentify the desktop domain as being the user domain.

Read the following topics next:

- Integrating Linux Desktops with Active Directory
- Setting Up Single Sign-On for Linux Desktops
- Set Up Smart Card Redirection for Linux Desktops
- Set Up True SSO for Linux Desktops

Integrating Linux Desktops with Active Directory

Multiple solutions exist to integrate Linux distributions with Microsoft Active Directory (AD). Horizon Agent for Linux has no dependency on which solution is used.

Note For ease of deployment, if available for your Linux distribution, use System Security Services Daemon (SSSD) Authentication.

The following solutions are known to work for a Linux virtual machine running Horizon Agent.

- OpenLDAP Pass-through Authentication supports integration with Active Directory for desktops running any Linux distribution supported by Horizon Agent.

  Note For OpenLDAP Pass-through Authentication, you can perform the configuration in a template virtual machine. No additional steps are required in the cloned virtual machines.

- System Security Services Daemon (SSSD) Authentication supports offline domain join with Active Directory for instant-cloned desktops running the following Linux distributions.
  - Ubuntu 20.04/22.04
  - Debian 10.x/11.x/12.x
  - RHEL 7.9/8.x/9.x
  - Rocky Linux 8.x/9.x
  - CentOS 7.9
  - SLED/SLES 15.x
- PowerBroker Identity Services Open (PBISO) Authentication supports offline domain join with Active Directory for instant-cloned desktops running the following Linux distributions.
  - Ubuntu 20.04/22.04
  - RHEL 7.9
- Samba supports offline domain join with Active Directory for instant-cloned desktops running any Linux distribution supported by Horizon Agent. However, VMware recommends using SSSD Authentication for desktops running newer distributions and Samba only for desktops running older distributions, as described in the following note.

  Note

  - VMware recommends using the SSSD Authentication method (instead of Samba) for desktops running the following Linux distributions.
    - Ubuntu 20.04/22.04
    - Debian 11.x/12.x
    - RHEL 8.x/9.x
    - Rocky Linux 8.x/9.x
    - SLED/SLES 15.x
  - VMware recommends using the Samba method for desktops running the following Linux distributions.
    - Debian 10.x
    - RHEL/CentOS 7.9

Use OpenLDAP Server Pass-through Authentication for Linux Desktops

You can set up an OpenLDAP server and use the pass-through authentication (PTA) mechanism to verify the user credentials against Active Directory.

OpenLDAP Pass-through Authentication supports integration with Active Directory for desktops running any Linux distribution supported by Horizon Agent.

Note For OpenLDAP Pass-through Authentication, you can perform the configuration in a template virtual machine. No additional steps are required in the cloned virtual machines.

At a high level, the OpenLDAP Pass-through Authentication solution involves the following steps.

Procedure

1. To enable LDAPS (Lightweight Directory Access Protocol over SSL), install Certificate Services on the Active Directory.
2. Set up an OpenLDAP server.
3. Synchronize user information (except password) from the Active Directory to the OpenLDAP server.
4. Configure the OpenLDAP server to delegate password verification to a separate process such as `saslauthd`, which can perform password verification against the Active Directory.
5. Configure the Linux virtual machines to use an LDAP client to authenticate users with the OpenLDAP server.

Configure SSSD Offline Domain Join for Linux Desktops

The System Security Services Daemon (SSSD) authentication method is one of the supported solutions for performing an offline domain join on an instant-cloned Linux virtual machine (VM).

System Security Services Daemon (SSSD) Authentication supports offline domain join with Active Directory for instant-cloned desktops running the following Linux distributions.

- Ubuntu 20.04/22.04
- Debian 10.x/11.x/12.x
- RHEL 7.9/8.x/9.x
- Rocky Linux 8.x/9.x
- CentOS 7.9
- SLED/SLES 15.x

Use the guidelines described in the following procedure to offline domain-join an instant-cloned Linux VM to Active Directory (AD) using SSSD authentication.

Procedure

1 On the golden-image Linux VM, perform the domain join using SSSD authentication. Ensure that the golden image uses the same domain as the instant clones.

For detailed domain-join instructions, refer to the documentation for your Linux distribution.

- (Ubuntu) Go to https://ubuntu.com/server/docs and search for information related to SSSD and Active Directory.
- (RHEL/CentOS) Go to the Red Hat customer portal and find the documentation page for your release version. For example, you can find English documentation at https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/.
  - For RHEL 9.x, find the "Configuring authentication and authorization in RHEL" document and search for information related to SSSD.
  - For RHEL 8.x, find the "Integrating RHEL Systems Directly With Windows Active Directory" document and search for information related to connecting RHEL systems directly to AD using SSSD.
  - For RHEL/CentOS 7.x, find the "Windows Integration Guide" and search for information related to discovering and joining identity domains.
- (Rocky Linux) Go to the Rocky Linux documentation portal at https://docs.rockylinux.org/ and search for information related to SSSD.
- (SLED/SLES) Go to the SUSE documentation portal at https://documentation.suse.com/ and search for information related to integrating Linux and Active Directory environments.

2 Install the `krb5` support libraries.

- (Ubuntu) Run the following command.

  ```
  sudo apt-get install krb5-user
  ```

- (RHEL/CentOS and Rocky Linux) Run the following command.

  ```
  sudo yum install krb5-workstation
  ```

- (SLED/SLES) Run the following command sequence.

  ```
  sudo zypper install krb5-client
  sudo ln -s /usr/lib/mit/bin/ktutil /usr/bin/ktutil
  sudo ln -s /usr/lib/mit/bin/kvno /usr/bin/kvno
  ```

3 Install Horizon Agent for Linux, as described in Install Horizon Agent on a Linux Machine.

4. Modify the `/etc/sssd/sssd.conf` configuration file, using the following example as reference.

   Replace the placeholder values in the example with information specific to your configuration:

   - Replace *mydomain.com* with the DNS name of your AD domain.
   - Replace *MYDOMAIN.COM* with the DNS name of your AD domain, in all capital letters

   ```
   [sssd]
   domains = mydomain.com
   config_file_version = 2
   services = nss, pam

   [domain/mydomain.com]
   ad_domain = mydomain.com
   krb5_realm = MYDOMAIN.COM
   realmd_tags = manages-system joined-with-adcli
   cache_credentials = True
   id_provider = ad
   krb5_store_password_if_offline = True
   default_shell = /bin/bash
   ldap_id_mapping = True
   use_fully_qualified_names = False        #Use short name for user
   fallback_homedir = /home/%u@%d
   access_provider = ad
   ad_gpo_map_interactive = +gdm-vmwcred    #Add this line for SSO
   ad_gpo_access_control = permissive       #Deactivate GPO access control in the cloned VM
   ```

5. (RHEL/CentOS 7.x) Modify the `/etc/krb5.conf` configuration file to use only the rc4-hmac encryption algorithm.

   This is the only encryption algorithm supported when using SSSD authentication to domain-join an instant-cloned RHEL/CentOS 7.x VM.

   ```
   [libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}
    default_tkt_enctypes = rc4-hmac       #Add this line to use rc4-hmac encryption only
    default_tgs_enctypes = rc4-hmac       #Add this line to use rc4-hmac encryption only
   ```

6. To ensure that Horizon Agent recognizes the Linux VM as domain-joined using SSSD authentication, add the following line to the `/etc/vmware/viewagent-custom.conf` configuration file.

   ```
   OfflineJoinDomain=sssd
   ```

7. Restart the golden-image Linux VM and take a snapshot of the VM in vCenter Server.

Use Winbind Domain Join for Linux Desktops

The Winbind domain join solution, a Kerberos-based authentication solution, is another method of authenticating with Active Directory.

Use the following high-level steps to set up the Winbind domain join solution.

Procedure

1 Install the `winbind`, `samba`, and Kerberos packages on the Linux virtual machine.

2 Join the Linux desktop to Microsoft Active Directory (AD).

What to do next

If you use the Winbind Domain Join solution or another Kerberos authentication-based solution, join the template virtual machine to AD, and rejoin the cloned virtual machine to AD. For example, use the following command:

```
sudo /usr/bin/net ads join -U <domain_user>%<domain_password>
```

To run the domain rejoin command on a cloned virtual machine for the Winbind solution, include the command to a shell script and set the script path to the `RunOnceScript` option in the `/etc/vmware/viewagent-custom.conf` file. For more information, see Edit Configuration Files on a Linux Desktop.

Configure PBISO Authentication for Linux Desktops

The PowerBroker Identity Services Open (PBISO) authentication method is one of the supported solutions for performing an offline domain join.

PowerBroker Identity Services Open (PBISO) Authentication supports offline domain join with Active Directory for instant-cloned desktops running the following Linux distributions.

- Ubuntu 20.04/22.04
- RHEL 7.9

Use the following steps to join a Linux virtual machine to Active Directory (AD) using PBISO.

Prerequisites

To use PBISO with an instant-clone floating desktop pool, first install the `krb5-user` package on the source template VM. For example, on an Ubuntu VM, you can use the following installation command:

```
sudo apt-get install krb5-user
```

Procedure

1 Download PBISO 9.1.0 or later from the official PBISO download site.

2 Install PBISO on your Linux virtual machine. For example, on Ubuntu 20.04:

```
sudo ./pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

3 Install Horizon Agent for Linux.

4 Use PBISO to join the Linux virtual machine to the AD domain.

In the following example, **lxdc.vdi** is the domain name and **administrator** is the domain user name.

```
sudo domainjoin-cli join lxdc.vdi administrator
```

5 Set up the default configuration for domain users.

```
sudo /opt/pbis/bin/config UserDomainPrefix lxdc
sudo /opt/pbis/bin/config AssumeDefaultDomain true
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
sudo /opt/pbis/bin/config HomeDirTemplate %H/%U
```

6 Edit the /etc/pam.d/common-session file.

a Locate the line that says **session sufficient pam_lsass.so**.

b Replace that line with **session [success=ok default=ignore] pam_lsass.so**.

Note You must redo this step after you reinstall or update Horizon Agent.

7 Restart the Linux virtual machine and log in.

What to do next

Note

- If the /opt/pbis/bin/config AssumeDefaultDomain option is set to **false**, you must update the SSOUserFormat=<username>@<domain> setting in the /etc/vmware/viewagent-custom.conf file.
- When using instant-clone floating desktop pools, to avoid losing the DNS Server setting when you add the new network adapter to the cloned virtual machine, modify the resolv.conf file for your Linux system. Use the following example, for an Ubuntu system, as a guide for adding the necessary lines in the /etc/resolv.conf file.

```
nameserver 10.10.10.10
search mydomain.org
```

Configure Samba Offline Domain Join for Linux Desktops

To support SSO on an instant-cloned Linux virtual machine (VM) in a VMware Horizon 8 desktop environment, configure Samba on the golden-image Linux VM.

Samba supports offline domain join with Active Directory for instant-cloned desktops running any Linux distribution supported by Horizon Agent. However, VMware recommends using SSSD Authentication for desktops running newer distributions and Samba only for desktops running older distributions, as described in the following note.

Note

- VMware recommends using the SSSD Authentication method (instead of Samba) for desktops running the following Linux distributions.
  - Ubuntu 20.04/22.04
  - Debian 11.x/12.x
  - RHEL 8.x/9.x
  - Rocky Linux 8.x/9.x
  - SLED/SLES 15.x
- VMware recommends using the Samba method for desktops running the following Linux distributions.
  - Debian 10.x
  - RHEL/CentOS 7.9

Use the following procedure as an example for using Samba to offline domain join an instant-cloned Linux VM to Active Directory (AD). This procedure provides the steps for an Ubuntu system.

Procedure

1. On your golden-image Linux VM, install the `winbind` and `samba` packages.

   ```
   sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
   ```

   If needed, install any dependent libraries such as `smbfs` and `smbclient`.

2. Install the Samba `tdb-tools` package using the following command.

   ```
   sudo apt install tdb-tools
   ```

3. Install Horizon Agent for Linux. See Install Horizon Agent on a Linux Machine.

4. Edit the `/etc/samba/smb.conf` configuration file so that it has content similar to the following example.

   ```
   [global]
   security = ads
   realm = LAB.EXAMPLE.COM
   workgroup = LAB
   idmap uid = 10000-20000
   idmap gid = 10000-20000
   winbind enum users = yes
   ```

```
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

5. Edit the `/etc/krb5.conf` configuration file so that it has content similar to the following example.

```
[libdefaults]
default_realm = EXAMPLE.COM

krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms

kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

[realms]
EXAMPLE.COM = {
kdc = 10.111.222.33
}

[domain_realm]
example.com = EXAMPLE.COM
.example.com = EXAMPLE.COM
```

6. Edit the `/etc/nsswitch.conf` configuration file, as shown in the following example.

```
passwd: files winbind
group: files winbind
shadow: files winbind
gshadow: files
```

7. Verify that the host name is correct and that the system date and time are synchronized with your DNS system.

8. To inform Horizon Agent that the Linux VM is domain-joined using the Samba method, configure the following options in the `/etc/vmware/viewagent-custom.conf` file. Replace *YOURDOMAIN* with the NetBIOS name of your domain.

```
OfflineJoinDomain=samba

NetbiosDomain=YOURDOMAIN
```

9. Restart the golden-image Linux VM and log back in.

Use Realmd Join for RHEL or Rocky Linux 8.x Desktops

To ensure the operation of features such as single sign-on for a RHEL 8.x or Rocky Linux 8.x desktop, use the solution to join the base virtual machine to your Active Directory (AD) domain.

Procedure

1 Configure a fully qualified host name for the base virtual machine (VM).

For example, if **`rhel8`** is the unqualified host name of the VM and **`LXD.VDI`** is the AD domain, run the following command.

```
sudo hostnamectl set-hostname rhel8.lxd.vdi
```

2 Verify the network connection with the AD domain, as shown in the following example.

```
sudo realm discover -vvv LXD.VDI
```

3 Install the required dependency packages, as shown in the following example.

```
sudo dnf install -y sssd adcli samba-common-tools oddjob oddjob-mkhomedir
```

4 Join the AD domain, as shown in the following example.

```
sudo realm join -U Administrator LXD.VDI
```

5 Edit the `/etc/sssd/sssd.conf` so that it resembles the following example. Add `ad_gpo_map_interactive = +gdm-vmwcred` under the *[domain/domain name]* section.

```
[sssd]
domains = LXD.VDI
config_file_version = 2
services = nss, pam

[domain/LXD.VDI]
ad_domain = LXD.VDI
krb5_realm = LXD.VDI
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred
```

6 To ensure that the domain-join takes effect, restart the VM and log back in.

7. Verify that the domain users are configured correctly. The following example shows how to use the `id` command to return the configuration output from domain user **`zyc1`**.

   ```
   id zyc1

   uid=1084401403(zyc1) gid=1084400513(domain users) groups=1084400513(domain users)
   ```

8. Using the credentials of a domain user, verify that you can successfully log in to the VM.

   Note Horizon Agent only supports the X11 display server protocol for RHEL and Rocky Linux 8.x desktops.

Setting Up Single Sign-On for Linux Desktops

To set up single sign-on (SSO) for Linux desktops, you must perform some configuration steps.

The VMware Horizon 8 single sign-on module communicates with PAM (pluggable authentication modules) in Linux and does not depend on the method that you use to integrate the Linux virtual machine with Active Directory (AD). Horizon 8 SSO is known to work with the OpenLDAP and Winbind solutions that integrate Linux virtual machines with AD.

By default, SSO assumes that AD's sAMAccountName attribute is the login ID. To ensure that the correct login ID is used for SSO, you must perform the following configuration steps if you use the OpenLDAP or Winbind solution:

- For OpenLDAP, set `sAMAccountName` to `uid`.
- For Winbind, add the following statement to the configuration file `/etc/samba/smb.conf`.

  ```
  winbind use default domain = true
  ```

If users must specify the domain name to log in, you must set the `SSOUserFormat` option on the Linux desktop. For more information, see Edit Configuration Files on a Linux Desktop. SSO always uses the short domain name in upper case. For example, if the domain is `mydomain.com`, SSO uses MYDOMAIN as the domain name. Therefore, you must specify MYDOMAIN when setting the `SSOUserFormat` option. Regarding short and long domain names, the following rules apply:

- For OpenLDAP, you must use short domain names in upper case.
- Winbind supports both long and short domain names.

AD supports special characters in login names, but Linux does not. Therefore, do not use special characters in login names when setting up SSO.

In AD, if a user's `UserPrincipalName` (UPN) attribute and `sAMAccount` attribute do not match, and the user logs in with the UPN, SSO fails. For example, if you have a user, `juser` in AD `mycompany.com`, but the user's UPN is set to `juser123@mycompany.com` instead of `juser@mycompany.com`, SSO fails. The workaround is for the user to log in using the name that is stored in `sAMAccount`. For example, `juser`.

Horizon Agent does not require the user name to be case-sensitive. You must ensure that the Linux operating system can handle case-insensitive user names.

- For Winbind, the user name is case-insensitive by default.
- For OpenLDAP, Ubuntu uses NSCD to authenticate users and is case-insensitive by default.
- RHEL, Rocky Linux, and CentOS use SSSD to authenticate users and the default is case-sensitive. To change the setting, edit the file `/etc/sssd/sssd.conf` and add the following line in the `[domain/default]` section:

  ```
  case_sensitive = false
  ```

If your Linux virtual machine has multiple desktop environments installed on it, refer to Desktop Environment to select the desktop environment to use with SSO.

Set Up Smart Card Redirection for Linux Desktops

When you enable smart card redirection on a Linux desktop, a user can authenticate into the desktop using a smart card reader connected to the local client system. To set up smart card redirection, you must perform some configuration steps.

Overview of Smart Card Redirection

Smart card redirection is supported on desktops based on virtual machines running the following Linux distributions:

- RHEL 7.x/8.x/9.x
- Rocky Linux 8.x/9.x
- Ubuntu 20.04/22.04
- Debian 10.x/11.x/12.x
- SLED/SLES 15.x

When you install Horizon Agent, you must specifically select the smart card redirection component because the component is not selected by default. For more information, see Command-line Options for Installing Horizon Agent for Linux .

The smart card redirection feature depends on the PC/SC Lite library (pcsc-lite) to establish communication with applications on the desktop. You can use either the default PC/SC Lite library included with your desktop's distribution or a custom-built PC/SC Lite library. If you use a custom library, you must configure the `/etc/vmware/config` file to match the reader context and message body settings of your custom PC/SC Lite library.

If you enable the smart card redirection feature on a virtual machine, vSphere Client's USB redirection does not work with the smart card.

Smart card redirection supports only one smart card reader at a time. This feature does not work if two or more readers are connected to the client system.

Smart card redirection supports only one certificate on the card. If more than one certificate is on the card, the one in the first slot is used and the others are ignored. This behavior is a Linux limitation.

The smart card single sign-on (SSO) feature allows users to launch desktop sessions without entering their smart card credentials. The `/etc/vmware/viewagent-greeter.conf` configuration file contains settings related to the smart card SSO feature, as well as to the VMware greeter when SSO is deactivated . For more information, see Edit Configuration Files on a Linux Desktop.

Note Smart card redirection supports the use of PIV cards to authenticate into Linux desktops. When you use Horizon Client for Linux to authenticate the broker with a PIV card, you must configure the PIV smart card with TLSv1.2 support to avoid receiving an SSL error.

Configuring Smart Card Redirection

To configure smart card redirection, perform the following tasks.

1 Set up the smart card by following the instructions from the smart card vendor.

2 Integrate the base virtual machine with an Active Directory domain, following the procedure for your Linux distribution.

3 Configure smart card redirection on the base virtual machine, following the procedure for your Linux distribution.

4 If you are using a custom PC/SC Lite library, configure the `pcscd.maxReaderContext` and `pcscd.readBody` options in the `/etc/vmware/config` file. See Edit Configuration Files on a Linux Desktop.

Configure Smart Card Redirection for RHEL and Rocky Linux 9.x/8.x Desktops

To set up smart card direction for RHEL and Rocky Linux 9.x/8.x desktops, first integrate the source virtual machine with an Active Directory domain. Then install the necessary libraries and root CA certificate before installing Horizon Agent.

Integrate a RHEL or Rocky Linux 9.x/8.x VM with AD for Smart Card Redirection

Use the following procedure to integrate a RHEL or Rocky Linux 9.x/8.x virtual machine (VM) with an Active Directory (AD) domain for smart card redirection.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
rhelsc.domain.com	Fully qualified host name of your VM

Placeholder Value	Description
rhelsc	Unqualified host name of your VM
domain.com	DNS name of your AD domain
DOMAIN.COM	DNS name of your AD domain, in all capital letters
DOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
dnsserver.domain.com	Host name of your AD server

Procedure

1 On the VM, do the following.

   a Configure network and DNS settings as required by your organization.

   b Turn off **IPv6**.

   c Turn off **Automatic DNS**.

2 Configure the `/etc/hosts` configuration file, so that it resembles the following example.

```
127.0.0.1        rhelsc.domain.com rhelsc localhost localhost.localdomain localhost4
localhost4.localdomain4
::1              localhost localhost.localdomain localhost6 localhost6.localdomain6

dns_IP_ADDRESS   dnsserver.domain.com
```

3 Configure the `/etc/resolv.conf` configuration file, so that it resembles the following example.

```
# Generated by NetworkManager
search domain.com
nameserver dns_IP_ADDRESS
```

4 Install the packages required for the AD integration.

```
sudo yum install -y samba-common-tools oddjob-mkhomedir
```

5 Specify the system identity and authentication sources.

```
sudo authselect select sssd with-smartcard with-mkhomedir
```

6 Start the `oddjobd` service.

- (RHEL or Rocky Linux 8.x) Run the following commands.

```
sudo systemctl enable oddjobd.service
sudo systemctl start oddjobd.service
```

- (RHEL or Rocky Linux 9.x) Run the following command.

  ```
  sudo systemctl enable --now oddjobd.service
  ```

7 To support smart card authentication, create the `/etc/sssd/sssd.conf` file.

```
sudo touch /etc/sssd/sssd.conf
sudo chmod 600 /etc/sssd/sssd.conf
sudo chown root:root /etc/sssd/sssd.conf
```

8 Add the required content to `/etc/sssd/sssd.conf`, as shown in the following example. Under the **`[pam]`** section, specify **`pam_cert_auth = True`**.

```
[sssd]
config_file_version = 2
domains = domain.com
services = nss, pam, pac

[domain/DOMAIN.COM]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
cache_credentials = true

[pam]
pam_cert_auth = True
```

9 (RHEL or Rocky Linux 8.x) Enable the `sssd` service.

```
sudo systemctl enable sssd.service
sudo systemctl start sssd.service
```

10 Edit the `/etc/krb5.conf` configuration file so that it resembles the following example.

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = /etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_realm = DOMAIN.COM
```

```
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 DOMAIN.COM = {
     kdc = dnsserver.domain.com
     admin_server = dnsserver.domain.com
     default_domain = dnsserver.domain.com
     pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
     pkinit_cert_match = <KU>digitalSignature
     pkinit_kdc_hostname = dnsserver.domain.com
 }

[domain_realm]
 .domain.com = DOMAIN.COM
 domain.com = DOMAIN.COM
```

11 Edit the `/etc/samba/smb.conf` configuration file so that it resembles the following example.

```
[global]
        workgroup = DOMAIN
        security = ads
        passdb backend = tdbsam
        printing = cups
        printcap name = cups
        load printers = yes
        cups options = raw
        password server = dnsserver.domain.com
        realm = DOMAIN.COM
        idmap config * : range = 16777216-33554431
        template homedir =/home/DOMAIN/%U
        template shell = /bin/bash
        kerberos method = secrets and keytab

[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = No
        read only = No
        inherit acls = Yes

[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @printadmin root
        force group = @printadmin
        create mask = 0664
        directory mask = 0775
```

12. Join the AD domain, as shown in the following example.

    ```
    sudo net ads join -U AdminUser
    ```

    Running the `join` command returns output similar to the following example.

    ```
    Enter AdminUser's password:
    Using short domain name -- DOMAIN
    Joined 'rhelsc' to dns domain 'domain.com'
    ```

13. Verify that the VM is successfully joined to the AD domain.

    ```
    sudo net ads testjoin
    ```

    A successful AD join returns the following output.

    ```
    Join is OK
    ```

What to do next

Configure Smart Card Redirection on a RHEL or Rocky Linux 9.x/8.x VM

Configure Smart Card Redirection on a RHEL or Rocky Linux 9.x/8.x VM

To configure smart card redirection on a RHEL or Rocky Linux 9.x/8.x virtual machine (VM), install the libraries on which the feature depends and the root Certificate Authority (CA) certificate to support the trusted authentication of smart cards.

Prerequisites

- Integrate a RHEL or Rocky Linux 9.x/8.x VM with AD for Smart Card Redirection
- To use the smart card single sign-on (SSO) feature in FIPS mode, ensure that you have completed all the steps described in Configure a FIPS-compliant Linux Machine. You must add the trusted CA certificate for VMwareBlastServer to `/etc/vmware/ssl/rui.crt` and add the key paired with `rui.crt` to `/etc/vmware/ssl/rui.key`.

Procedure

1. Install the required libraries.

    ```
    sudo yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools
    ```

2. Enable the `pcscd` service.

    ```
    sudo systemctl enable pcscd
    sudo systemctl start pcscd
    ```

3 Make sure that the `/etc/sssd/sssd.conf` configuration file contains the following lines, which enable smart card authentication.

```
[pam]
pam_cert_auth = True
```

4 Copy the required CA certificate to `/etc/sssd/pki/sssd_auth_ca_db.pem`.

```
sudo openssl x509 -inform der -in certificate.cer -out certificate.pem
sudo cp certificate.pem /etc/sssd/pki/sssd_auth_ca_db.pem
```

5 To verify the status of the smart card, run the following `pkcs11-tool` commands and confirm that they return the correct output.

```
sudo pkcs11-tool -L

sudo pkcs11-tool --login -O

sudo pkcs11-tool --test --login
```

6 To support the smart card SSO feature and the VMware greeter when SSO is deactivated, configure the `/etc/vmware/viewagent-greeter.conf` file. See Edit Configuration Files on a Linux Desktop.

7 Install the Horizon Agent package, with smart card redirection enabled.

- If using the `.rpm` installer:

  1 Run the installer to install Horizon Agent with the default feature options.

  ```
  sudo rpm -ivh VMware-horizonagent-linux-YYMM-y.y.y-xxxxxxx.el8.x86_64.rpm
  ```

  2 To add the smart card redirection feature, run the `ViewSetup.sh` script.

  ```
  sudo /usr/lib/vmware/viewagent/bin/ViewSetup.sh -m yes
  ```

- If using the `.tar.gz` installer, run the installer with the parameter to enable smart card redirection:

  ```
  sudo ./install_viewagent.sh -m yes
  ```

Note If you get an error message instructing you to install the default PC/SC Lite library, uninstall the custom PC/SC Lite library that is currently present on the machine and install the default PC/SC Lite library using the following command.

```
sudo yum reinstall pcsc-lite-libs pcsc-lite
```

You can then run the Horizon Agent installer.

8 If you are using a custom PC/SC Lite library, configure the `pcscd.maxReaderContext` and `pcscd.readBody` options in the `/etc/vmware/config` file.

   See Edit Configuration Files on a Linux Desktop.

9 Restart the virtual machine and log back in.

Configure Smart Card Redirection for RHEL 7.9 Desktops

To set up smart card direction for RHEL 7.9 desktops, first integrate the RHEL 7.9 virtual machine with an Active Directory domain. Then install the necessary libraries and root CA certificate before installing Horizon Agent.

Integrate a RHEL 7.9 VM with AD for Smart Card Redirection

To support smart card redirection on RHEL 7.9 desktops, integrate the base virtual machine (VM) with your Active Directory (AD) domain using the Samba and Winbind solutions.

Use the following procedure to integrate a RHEL 7.9 VM with your AD domain for smart card redirection.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server

Procedure

1 On the RHEL 7.9 VM, install the required packages.

```
sudo yum install nscd samba-winbind krb5-workstation pam_krb5 samba-winbind-clients
authconfig-gtk
```

2 Edit the network settings for your system connection. Open the NetworkManager control panel and navigate to the **IPv4 Settings** for your system connection. For IPv4 Method, select **Automatic (DHCP)** . In the **DNS** text box, enter the IP address of your DNS name server. Then click **Apply**.

3 Run the following command and verify that it returns the Fully Qualified Domain Name (FQDN) of the RHEL 7.9 VM.

```
hostname -f
```

4 Edit the `/etc/resolv.conf` configuration file, as shown in the following example.

```
search mydomain.com
nameserver dns_IP_ADDRESS
```

5 Edit the `/etc/krb5.conf` configuration file, as shown in the following example.

```
[libdefaults]
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_realm = MYDOMAIN.COM
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
            default_domain = ads-hostname
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

6 Edit the `/etc/samba/smb.conf` configuration file, as shown in the following example.

```
[global]
      workgroup = MYDOMAIN
      password server = ads-hostname
      realm = MYDOMAIN.COM
      security = ads
      idmap config * : range = 16777216-33554431
      template homedir =/home/MYDOMAIN/%U
      template shell = /bin/bash
      kerberos method = secrets and keytab
      winbind use default domain = true
      winbind offline logon = false
      winbind refresh tickets = true

      passdb backend = tdbsam
```

7 Open the `authconfig-gtk` tool and configure settings as follows.

   a Select the **Identity & Authentication** tab. For User Account Database, select **Winbind**.

   b Select the **Advanced Options** tab, and select the **Create home directories on the first login** check box.

   c Select the **Identity & Authentication** tab and then click **Join Domain**. At the alert asking you to save changes, click **Save**.

   d When prompted, enter the user name and password of the domain administrator, and click **OK**.

   The RHEL 7.9 VM is joined to the AD domain.

8 Set up ticket caching on PAM Winbind. Edit the `/etc/security/pam_winbind.conf` configuration file so that it includes the lines shown in the following example.

```
[global]

# authenticate using kerberos
;krb5_auth = yes

# create homedirectory on the fly
;mkhomedir = yes
```

9 Restart the Winbind service.

```
sudo service winbind restart
```

10 To verify the AD join, run the following commands and ensure that they return the correct output.

```
sudo net ads testjoin

sudo net ads info
```

11 Restart the RHEL 7.9 VM and log back in.

What to do next

Set Up Smart Card Redirection on a RHEL 7.9 VM

Set Up Smart Card Redirection on a RHEL 7.9 VM

To configure smart card redirection on a RHEL 7.9 virtual machine (VM), install the libraries on which the feature depends and the root Certificate Authority (CA) certificate required for authentication. In addition, you must edit some configuration files to complete the authentication setup.

To set up smart card redirection on a RHEL 7.9 VM, use the following procedure.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server

Note If you use the vSphere console to log in to a RHEL 7.9. VM that has Horizon Agent installed and smart card redirection enabled, you might experience a delayed logout time of two minutes or longer. This delayed logout only occurs from the vSphere console. The RHEL 7.9 logout experience from Horizon Client is not affected.

Prerequisites

Integrate a RHEL 7.9 VM with AD for Smart Card Redirection

Procedure

1 Install the required libraries.

```
sudo yum install nss-tools nss-pam-ldapd esc pam_pkcs11 pam_krb5 opensc pcsc-lite-ccid
authconfig
      authconfig-gtk krb5-libs krb5-workstation krb5-pkinit pcsc-lite pcsc-lite-libs
```

2 Install a root CA certificate.

   a Download a root CA certificate and save it to `/tmp/certificate.cer` on your desktop. See How to Export Root Certification Authority Certificate.

   b Locate the root CA certificate that you downloaded, and transfer it to a `.pem` file.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

   c Use the `certutil` command to install the root CA certificate to the system database `/etc/pki/nssdb`.

   Replace "root CA cert" in the following example command with the name of the root CA certificate in the system database.

```
sudo certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/
certificate.pem
```

3. Navigate to **Applications > Sundry > Authentication**, select the **Enable smart card support** check box, and click **Apply**.

4. Edit the `module` setting in the `/etc/pam_pkcs11/pam_pkcs11.conf` configuration file, as shown in the following example.

```
use_pkcs11_module = coolkey;
...
pkcs11_module coolkey {
      module = libcoolkeypk11.so;
      description = "Cool Key";
      slot_num = 0;
      nss_dir = /etc/pki/nssdb;
      cert_policy = ca, signature;
}
```

5. Edit the `/etc/pam_pkcs11/cn_map` file so that it includes content similar to the following example. For the specific content to include, refer to the user information listed in the smart card certificate.

```
user sc -> user-sc
```

6. Edit the `/etc/krb5.conf/` configuration file, as shown in the following example.

```
[libdefaults]
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_realm = MYDOMAIN.COM
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
            default_domain = ads-hostname
            pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
            pkinit_cert_match = <KU>digitalSignature
            pkinit_kdc_hostname = ads-hostname
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

7. If the VM is running the MATE desktop environment, add the line `auth include smartcard-auth` to the beginning of the `/etc/pam.d/mate-screensaver` as shown in the following example.

   ```
   #%PAM-1.0

   # Fedora Core
   auth include smartcard-auth
   auth        include      system-auth
   auth        optional     pam_gnome_keyring.so
   account     include      system-auth
   password    include      system-auth
   session     include      system-auth
   ```

   You must perform this configuration to ensure that users can unlock the screen when logging in with a smart card.

8. To support the smart card single sign-on (SSO) feature and the VMware greeter when SSO is deactivated, configure the `/etc/vmware/viewagent-greeter.conf` file. See Edit Configuration Files on a Linux Desktop.

9. Restart the PC/SC daemon.

   ```
   sudo chkconfig pcscd on
   sudo service pcscd start
   ```

10. Install the Horizon Agent package, with smart card redirection enabled.

    ```
    sudo ./install_viewagent.sh -m yes
    ```

    Note If you get an error message instructing you to install the default PC/SC Lite library, uninstall the custom PC/SC Lite library that is currently present on the machine and install the default PC/SC Lite library using the following command.

    ```
    yum reinstall pcsc-lite-libs pcsc-lite
    ```

    You can then run the Horizon Agent installer.

11. If you are using a custom PC/SC Lite library, configure the `pcscd.maxReaderContext` and `pcscd.readBody` options in the `/etc/vmware/config` file.

    See Edit Configuration Files on a Linux Desktop.

12. Restart the VM and log back in.

Configure Smart Card Redirection for Ubuntu/Debian Desktops

To set up smart card direction for desktops running Ubuntu or Debian, first integrate the Ubuntu/Debian virtual machine with an Active Directory domain. Then install the necessary libraries and root Certificate Authority (CA) certificate before installing Horizon Agent.

Integrate an Ubuntu/Debian VM with AD for Smart Card Redirection

To support smart card redirection on Ubuntu/Debian desktops, integrate the base virtual machine (VM) with an Active Directory (AD) domain using the Samba and Winbind solutions.

Use the following procedure to integrate an Ubuntu/Debian VM with an AD domain for smart card redirection.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server
ads-hostname.mydomain.com	Fully qualified domain name (FQDN) of your AD server
mytimeserver.mycompany.com	DNS name of your NTP time server
AdminUser	User name of the VM administrator

Procedure

1 On the Ubuntu/Debian VM, define the host name of the VM by editing the `/etc/hostname` configuration file.

2 Configure DNS.

   a Add the DNS server name and IP address to the `/etc/hosts` configuration file.

   b Add your DNS name server's IP address and the DNS name of your AD domain to the `/etc/network/interfaces` configuration file, as shown in the following example.

```
dns-nameservers dns_IP_ADDRESS
dns-search mydomain.com
```

3 Install the `resolvconfig` package.

   a Run the installation command.

   ```
   sudo apt-get install -y resolvconf
   ```

   Allow the system to install the package and reboot.

   b Verify your DNS configuration in the `/etc/resolv.conf` file by running the following command.

   ```
   sudo cat /etc/resolv.conf
   ```

   Verify that the command returns output similar to the following example.

   ```
   nameserver dns_IP_ADDRESS
   search mydomain.com
   ```

4 Configure network time synchronization.

   a Install the `ntpdate` package.

   ```
   sudo apt-get install -y ntpdate
   ```

   b Add the NTP server information to the `/etc/systemd/timesyncd.conf` configuration file, as shown in the following example.

   ```
   [Time]
   NTP=mytimeserver.mycompany.com
   ```

5 Restart the NTP service.

```
sudo service ntpdate restart
```

6 Install the required AD join packages.

   a Run the installation command.

   ```
   sudo apt-get install -y samba krb5-config krb5-user winbind libpam-winbind
       libnss-winbind
   ```

   b At the installation prompt asking for the default Kerberos realm, enter the DNS name of your AD domain in capital letters (for example, `MYDOMAIN.COM`). Then select **Ok**.

7 Edit the `/etc/krb5.conf` configuration file, as shown in the following example.

```
[libdefaults]
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_realm = MYDOMAIN.COM
```

```
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname.mydomain.com
            admin_server = ads-hostname.mydomain.com
            default_domain = ads-hostname.mydomain.com
            pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
            pkinit_cert_match = <KU>digitalSignature
            pkinit_kdc_hostname = ads-hostname.mydomain.com
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

8 To verify the Kerberos certification, run the following commands.

```
sudo kinit Administrator@MYDOMAIN.COM

sudo klist
```

Verify that the commands return output similar to the following example.

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MYDOMAIN.COMValid starting        Expires
Service principal
2019-05-27T17:12:03   2019-05-28T03:12:03    krbtgt/MYDOMAIN.COM@MYDOMAIN.COM
        renew until 2019-05-28T17:12:03
```

9 Edit the `/etc/samba/smb.conf` configuration file, as shown in the following example.

```
[global]
        workgroup = MYDOMAIN
        usershare allow guests = NO
        idmap gid = 10000-20000
        idmap uid = 10000-20000
        kerberos method = secrets and keytab
        realm = MYDOMAIN.COM
        security = ADS
        template homedir = /home/%D/%U
        template shell = /bin/bash
        winbind use default domain=true
        winbind offline logon = yes
        winbind refresh tickets = yes
```

10 Join the AD domain, and check the integration.

   a Run the AD join commands.

```
sudo net ads join -U AdminUser@mydomain.com
sudo systemctl stop samba-ad-dc
sudo systemctl enable smbd nmbd winbind
sudo systemctl restart smbd nmbd winbind
```

   b Modify the `/etc/nsswitch.conf` configuration file, as shown in the following example.

```
passwd:    compat systemd winbind
group:     compat systemd winbind
shadow:    compat
gshadow:   files
```

   c To check the results of the AD join, run the following commands and verify that they return the correct output.

```
sudo wbinfo -u

sudo wbinfo -g
```

   d To check the Winbind Name Service Switch, run the following commands and verify that they return the correct output.

```
sudo getent group|grep 'domain admins'

sudo getent passwd|grep 'ads-hostname'
```

11 Enable all PAM profiles.

```
pam-auth-update
```

In the PAM Configuration screen, select all the PAM profiles, including **Create home directory on login**, and then select **Ok**.

What to do next

Set Up Smart Card Redirection on an Ubuntu/Debian VM

Set Up Smart Card Redirection on an Ubuntu/Debian VM

To configure smart card redirection on an Ubuntu/Debian virtual machine (VM), install the libraries on which the feature depends and the root Certificate Authority (CA) certificate to support the trusted authentication of smart cards. In addition, you must edit some configuration files to complete the authentication setup.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server
ads-hostname.mydomain.com	Fully qualified domain name (FQDN) of your AD server
mytimeserver.mycompany.com	DNS name of your NTP time server
AdminUser	User name of the VM administrator

Prerequisites

Integrate an Ubuntu/Debian VM with AD for Smart Card Redirection

Procedure

1 Install the required libraries on the Ubuntu/Debian VM.

```
sudo apt-get install -y pcscd pcsc-tools pkg-config libpam-pkcs11 opensc libengine-pkcs11-
openssl libnss3-tools
```

2 Install a root CA certificate.

a Download a root CA certificate and save it to `/tmp/certificate.cer` on the Ubuntu VM. See How to Export Root Certification Authority Certificate.

b Locate the root CA certificate that you downloaded, and transfer it to a `.pem` file.

```
sudo openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

c Copy the root CA certificate to the `/etc/pam_pkcs11/cacerts` directory.

```
sudo cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

3 Create a `pkcs11` hash file.

```
sudo chmod a+r certificate.pem
sudo pkcs11_make_hash_link
```

4 Configure the `pam_pkcs11` library.

a Create a `pam_pkcs11.conf` file using default example content.

- (Ubuntu 20.04, Debian 10.x) Run the following command sequence.

```
sudo mkdir /etc/pam_pkcs11
sudo zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz |
tee /etc/pam_pkcs11/pam_pkcs11.conf
```

- (Ubuntu 20.04.1 and later, Ubuntu 22.04, Debian 11.x/12.x) Run the following command sequence.

```
sudo mkdir /etc/pam_pkcs11
sudo cat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example | tee /etc/
pam_pkcs11/pam_pkcs11.conf
```

b Edit the `/etc/pam_pkcs11/pam_pkcs11.conf` file as shown in the following example.

```
use_pkcs11_module = opensc;
...
pkcs11_module opensc {
     module = /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so;
     description = "OpenSC PKCS#11 module";
     slot_num = 0;
     ca_dir = /etc/pam_pkcs11/cacerts;
     crl_dir = /etc/pam_pkcs11/crls;
     support_threads = false;
     cert_policy = ca,signature;
     token_type = "Smart card";
}
...
use_mappers = cn, null;
...
mapper cn {
     debug = false;
     module = internal;
     ignorecase = true;
     mapfile = file:///etc/pam_pkcs11/cn_map;
}
```

c Edit the `/etc/pam_pkcs11/cn_map` file so that it includes the following line.

```
Common name -> Login ID
```

5 Edit the `/etc/pam.d/gdm-password` configuration file. Place the `pam_pkcs11.so` authorization line before the `common-auth` line, as shown in the following example.

```
#%PAM-1.0
auth    requisite       pam_nologin.so
auth    required        pam_succeed_if.so user != root quiet_success
auth sufficient
pam_pkcs11.so
```

```
@include common-auth
auth    optional        pam_gnome_keyring.so
@include common-account
```

6 To verify the smart card hardware and the certificates installed on the smart card, run the following commands.

```
sudo pcsc_scan
sudo pkcs11_listcerts
sudo pkcs11_inspect
```

7 To support the smart card SSO feature and the VMware greeter when SSO is deactivated, configure the `/etc/vmware/viewagent-greeter.conf` file. See Edit Configuration Files on a Linux Desktop.

8 Install the Horizon Agent package, with smart card redirection enabled.

```
sudo ./install_viewagent.sh -m yes
```

Note If you get an error message instructing you to install the default PC/SC Lite library, uninstall the custom PC/SC Lite library that is currently present on the machine and install the default PC/SC Lite library using the following command.

```
sudo apt-get install --reinstall pcscd libpcsclite1
```

You can then run the Horizon Agent installer.

9 If you are using a custom PC/SC Lite library, configure the `pcscd.maxReaderContext` and `pcscd.readBody` options in the `/etc/vmware/config` file.

See Edit Configuration Files on a Linux Desktop.

10 Restart the Ubuntu VM and log back in.

Configure Smart Card Redirection for SLED/SLES Desktops

To set up smart card direction for SLED/SLES desktops, first integrate the base virtual machine with an Active Directory domain. Then install the necessary libraries and root Certificate Authority (CA) certificate before installing Horizon Agent.

Integrate a SLED/SLES VM with AD for Smart Card Redirection

To support smart card redirection on SLED/SLES desktops, integrate the base virtual machine (VM) with an Active Directory (AD) domain using the Samba and Winbind solutions.

Use the following procedure to integrate a SLED/SLES VM with an AD domain for smart card redirection.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server
ads-hostname.mydomain.com	Fully qualified domain name (FQDN) of your AD server
mytimeserver.mycompany.com	DNS name of your NTP time server
AdminUser	User name of the VM administrator

Prerequisites

Verify that the SLED/SLES VM meets the system requirements described in Set Up Smart Card Redirection for Linux Desktops.

Procedure

1 Configure the network settings for the SLED/SLES VM.

   a Define the host name of the VM by editing the `/etc/hostname` and `/etc/hosts` configuration files.

   b Configure the DNS server IP address, and turn off **Automatic DNS**. For a SLES VM, also turn off **Change Hostname via DHCP**.

   c To configure network time synchronization, add your NTP server information to the `/etc/ntp.conf` file, as shown in the following example.

   ```
   server mytimeserver.mycompany.com
   ```

2 Install the required AD join packages.

```
sudo zypper in krb5-client samba-winbind
```

3 Update the krb5 library, as shown in the following example.

```
sudo zypper up krb5
```

4 Edit the required configuration files.

a Edit the `/etc/samba/smb.conf` file, as shown in the following example.

```
[global]
        workgroup = MYDOMAIN
        usershare allow guests = NO
        idmap gid = 10000-20000
        idmap uid = 10000-20000
        kerberos method = secrets and keytab
        realm = MYDOMAIN.COM
        security = ADS
        template homedir = /home/%D/%U
        template shell = /bin/bash
        winbind use default domain=true
        winbind offline logon = yes
        winbind refresh tickets = yes
[homes]
        ...
```

b Edit the `/etc/krb5.conf` file, as shown in the following example.

```
[libdefaults]
        default_realm = MYDOMAIN.COM
        clockskew = 300

[realms]
        MYDOMAIN.COM = {
                kdc = ads-hostname.mydomain.com
                default_domain = mydomain.com
                admin_server = ads-hostname.mydomain.com
        }

[logging]
        kdc = FILE:/var/log/krb5/krb5kdc.log
        admin_server = FILE:/var/log/krb5/kadmind.log
        default = SYSLOG:NOTICE:DAEMON

[domain_realm]
        .mydomain.com = MYDOMAIN.COM
        mydomain.com = MYDOMAIN.COM

[appdefaults]
        pam = {
                ticket_lifetime = 1d
                renew_lifetime = 1d
                forwardable = true
                proxiable = false
                minimum_uid = 1
        }
```

c Edit the `/etc/security/pam_winbind.conf` file, as shown in the following example.

```
cached_login = yes
krb5_auth = yes
krb5_ccache_type = FILE
```

d Edit the `/etc/nsswitch.conf` file, as shown in the following example.

```
passwd: compat winbind
group: compat winbind
```

5 Join the AD domain, as shown in the following example.

```
sudo net ads join -U AdminUser
```

6 Enable the Winbind service.

a To enable and start Winbind, run the following sequence of commands.

```
sudo pam-config --add --winbind
sudo pam-config -a --mkhomedir
sudo systemctl enable winbind
sudo systemctl start winbind
```

b To ensure that AD users can log in to desktops without having to restart the Linux server, run the following sequence of commands.

```
sudo systemctl stop nscd
sudo nscd -i passwd
sudo nscd -i group
sudo systemctl start nscd
```

7 To confirm the success of the AD join, run the following commands and check that they return the correct output.

```
sudo wbinfo -u
sudo wbinfo -g
```

What to do next

Proceed to Set Up Smart Card Redirection on a SLED/SLES VM.

Set Up Smart Card Redirection on a SLED/SLES VM

To configure smart card redirection on a SLED/SLES virtual machine (VM), install the libraries on which the feature depends and the root Certificate Authority (CA) certificate to support the trusted authentication of smart cards. In addition, you must edit some configuration files to complete the authentication setup.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server
ads-hostname.mydomain.com	Fully qualified domain name (FQDN) of your AD server
mytimeserver.mycompany.com	DNS name of your NTP time server
AdminUser	User name of the VM administrator

Prerequisites

Complete the steps described in Integrate a SLED/SLES VM with AD for Smart Card Redirection.

Procedure

1 Install the PAM library and other required packages.

```
sudo zypper install pam_pkcs11 mozilla-nss mozilla-nss-tools pcsc-lite pcsc-ccid opensc
pcsc-tools
```

You might need to enable extensions like PackageHub to install all the preceding packages.

2 Install a root CA certificate.

a Download a root CA certificate and save it to `/tmp/certificate.cer` on the system. See How to Export Root Certification Authority Certificate.

b Install trust anchors to the NSS database.

```
sudo mkdir /etc/pam_pkcs11/nssdb
sudo certutil -N -d /etc/pam_pkcs11/nssdb
sudo certutil -L -d /etc/pam_pkcs11/nssdb
sudo certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pam_pkcs11/nssdb
```

c Install the required drivers.

```
sudo modutil -add "opensc lib" -libfile /usr/lib64/opensc-pkcs11.so -dbdir /etc/
pam_pkcs11/nssdb/
```

3 Edit the `/etc/pam_pkcs11/pam_pkcs11.conf` file as shown in the following example.

```
use_pkcs11_module = opensc;
...
pkcs11_module opensc {
     module = /usr/lib64/opensc-pkcs11.so;
     description = "OpenSC PKCS#11 module";
     slot_num = 0;
     nss_dir = /etc/pam_pkcs11/nssdb;
     crl_dir = /etc/pam_pkcs11/crls;
     support_threads = false;
     cert_policy = ca,signature;
     token_type = "Smart card";
}
...
use_mappers = cn, null;
...
mapper cn {
     debug = false;
     module = internal;
     ignorecase = true;
     mapfile = file:///etc/pam_pkcs11/cn_map;
}
```

4 Edit the `/etc/pam_pkcs11/cn_map` configuration file so that it includes the following line.

```
ads-hostname -> ads-hostname
```

5 Modify the PAM configuration.

   a To make it possible to configure smart card authentication, first deactivate the `pam_config` tool.

   ```
   sudo find /etc/pam.d/ -type l -iname "common-*" -delete
   sudo for X in /etc/pam.d/common-*-pc; do cp -ivp $X ${X:0:-3}; done
   ```

   b Create a file named `common-auth-smartcard` under the `/etc/pam.d/` directory. Add the following content to the file.

   ```
   auth    required        pam_env.so
   auth    sufficient      pam_pkcs11.so
   auth    optional        pam_gnome_keyring.so
   auth    [success=1 default=ignore]      pam_unix.so nullok_secure try_first_pass
   auth    required        pam_winbind.so  use_first_pass
   ```

   c Replace the line `auth include common-auth` with the line `auth include common-auth-smartcard` in both of these files: `/etc/pam.d/gdm` and `/etc/pam.d/xscreensaver`.

6 To configure the pcscd service to start automatically after the VM restarts, edit the `pcscd.service` file.

   a Add the line `WantedBy=multi-user.target` to `/usr/lib/systemd/system/pcscd.service` so that the file resembles the following example.

   ```
   [Unit]
   Description=PC/SC Smart Card Daemon
   Requires=pcscd.socket

   [Service]
   ExecStart=/usr/sbin/pcscd --foreground --auto-exit
   ExecReload=/usr/sbin/pcscd --hotplug

   [Install]
   Also=pcscd.socket
   WantedBy=multi-user.target
   ```

   b After editing the `pcscd.service` file, run the following command.

   ```
   sudo systemctl enable pcscd
   ```

   Note If the pcscd service does not start after the VM restarts, the first login through pam_pkcs11 fails.

7 Turn off the firewall.

   ```
   sudo systemctl stop firewalld
   sudo systemctl disable firewalld
   ```

   Note Smart card redirection sometimes fails when the firewall is enabled.

8 To support the smart card SSO feature and the VMware greeter when SSO is deactivated, configure the `/etc/vmware/viewagent-greeter.conf` file. See Edit Configuration Files on a Linux Desktop.

9 Install the Horizon Agent package, with smart card redirection enabled.

   ```
   sudo ./install_viewagent.sh -m yes
   ```

   Note If you get an error message instructing you to install the default PC/SC Lite library, uninstall the custom PC/SC Lite library that is currently present on the machine and install the default PC/SC Lite library using the following command.

   ```
   sudo zypper install -f -y pcsc-lite libpcsclite1
   ```

   You can then run the Horizon Agent installer.

10. If you are using a custom PC/SC Lite library, configure the `pcscd.maxReaderContext` and `pcscd.readBody` options in the `/etc/vmware/config` file.

    See Edit Configuration Files on a Linux Desktop.

11. Restart the VM and log back in.

Set Up True SSO for Linux Desktops

The True Single Sign-on (True SSO) feature grants users access to a Linux remote desktop after they first log in to VMware Workspace ONE. Users can log in to VMware Workspace ONE using a smart card or RSA SecurID or RADIUS authentication, and then access remote Linux resources without entering their Active Directory credentials.

Overview of True SSO

If a user authenticates by using Active Directory (AD) credentials, the True SSO feature is not necessary. However, you can configure True SSO to be used even in this case, so that the desktop can support both AD credentials and True SSO.

When connecting to a Linux remote desktop, users can select to use either the native Horizon Client or HTML Access.

The `/etc/vmware/viewagent-greeter.conf` configuration file allows you to configure the behavior of the VMware greeter in cases where True SSO fails. See Edit Configuration Files on a Linux Desktop.

System Requirements for True SSO

True SSO is supported on single-session virtual desktops running the following Linux distributions:

- RHEL/CentOS 7.x
- RHEL 8.x/9.x
- Rocky Linux 8.x/9.x
- Ubuntu 20.04/22.04
- Debian 10.x/11.x/12.x
- SLED/SLES 15.x

True SSO is supported on multi-session published desktops and applications based on the following types of farms.

- Manual and automated instant-clone farms of Ubuntu 20.04/22.04, Debian 10.x, or RHEL Workstation 7.9 host machines that have been integrated with Active Directory using the Samba domain-join method.

- Manual and automated instant-clone farms of RHEL Workstation 8.x/9.x, Rocky Linux 8.x/9.x, or Debian 11.x/12.x host machines that have been integrated with Active Directory using the System Security Services Daemon (SSSD) domain-join method.

Configuring True SSO

To set up True SSO for Linux desktops, perform the following tasks.

1 Set up and configure True SSO in your VMware Horizon 8 environment. For more information, see the *Horizon 8 Administration* document.

2 Integrate the base virtual machine with an AD domain, following the procedure for your Linux distribution.

3 Configure True SSO on the base virtual machine, following the procedure for your Linux distribution.

Configure True SSO for RHEL and Rocky Linux 9.x/8.x Desktops

To support True SSO on a RHEL or Rocky Linux 9.x/8.x desktop, you must first integrate the base virtual machine (VM) with your Active Directory (AD) domain. Then you must modify certain configurations on the system to support the True SSO feature.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
MYDOMAIN	Name of your NetBIOS domain
dnsserver.mydomain.com	Name of your DNS server

Prerequisites

- Configure True SSO for Workspace ONE Access and Horizon Connection Server.
- Verify that the Active Directory (AD) server is resolvable by DNS on the base VM.
- Configure the host name of the VM.
- Configure the Network Time Protocol (NTP) on the VM.
- Get a root Certificate Authority (CA) certificate and save it to `/tmp/certificate.cer` on the VM. See How to Export Root Certification Authority Certificate.

  If a subordinate CA is also an issuing authority, then get the entire chain of root and subordinate CA certificates and save it to `/tmp/certificate.cer` on the VM.

- To use True SSO in FIPS mode, ensure that you have completed all the steps described in Configure a FIPS-compliant Linux Machine. You must add the trusted CA certificate for VMwareBlastServer to `/etc/vmware/ssl/rui.crt` and add the key paired with `rui.crt` to `/etc/vmware/ssl/rui.key`.

Procedure

1 On the base VM, verify the network connection to Active Directory.

```
sudo realm discover mydomain.com
```

2 Install the required dependency packages.

```
sudo yum install oddjob oddjob-mkhomedir sssd adcli samba-common-tools
```

3 Join the AD domain.

```
sudo realm join --verbose mydomain.com -U administrator
```

4 Install the root CA certificate or certificate chain.

   a Locate the root CA certificate or certificate chain that you downloaded, and transfer it to a PEM file.

   ```
   sudo openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
   ```

   b Copy the certificate to the `/etc/sssd/pki/sssd_auth_ca_db.pem` file.

   ```
   sudo cp /tmp/certificate.pem /etc/sssd/pki/sssd_auth_ca_db.pem
   ```

5 Modify the `/etc/sssd/sssd.conf` configuration file, as shown in the following example.

```
[sssd]
domains = mydomain.com
config_file_version = 2
services = nss, pam

[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = MYDOMAIN.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False             #Use short name for user
fallback_homedir = /home/%u@%d
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred         #Add this line for SSO

[pam]                                         #Add pam section for certificate logon
pam_cert_auth = True                          #Add this line to enable certificate logon
```

```
for system
pam_p11_allowed_services = +gdm-vmwcred       #Add this line to enable certificate logon
for VMware Horizon Agent

[certmap/mydomain.com/truesso]                #Add this section and following lines to set
match and map rule for certificate user
matchrule = <EKU>msScLogin
maprule = (|(userPrincipal={subject_principal})
(samAccountName={subject_principal.short_name}))
domains = mydomain.com
priority = 10
```

6 Modify the `/etc/krb5.conf` configuration file by setting the mode equal to `644`.

Note If you do not modify `/etc/krb5.conf` as specified, the True SSO feature might not work.

7 (RHEL or Rocky Linux 9.x) To ensure that TrueSSO works properly with instant-clone desktop pools, modify the following configurations.

Note You can skip these configurations if you are not using the VM for an instant-clone desktop pool.

a Run the command to explicitly allow the SHA-1 cryptographic policy.

```
sudo update-crypto-policies --set DEFAULT:SHA1
```

b Locate the root CA certificate or certificate chain that you downloaded earlier, and copy it to `/etc/pki/ca-trust/source/anchors/ca_cert.pem`. Then use the `update-ca-trust` command to enable legacy applications to read the trusted certificates.

```
sudo cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
sudo update-ca-trust
```

c Modify the `/etc/krb5.conf` file, as shown in the following example.

```
[realms]
     MYDOMAIN.COM = {
          kdc =  dnsserver.mydomain.com
          admin_server =  dnsserver.mydomain.com
          pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
          pkinit_kdc_hostname =  dnsserver.mydomain.com
          pkinit_eku_checking = kpServerAuth
     }
[domain_realm]
     .mydomain.com = MYDOMAIN.COM
     mydomain.com = MYDOMAIN.COM
```

8 Install the Horizon Agent package, with True SSO enabled.

```
sudo ./install_viewagent.sh -T yes
```

9 Modify the `/etc/vmware/viewagent-custom.conf` configuration file so that it includes the following line.

```
NetbiosDomain = MYDOMAIN
```

10 Restart the VM and log back in.

Configure True SSO for RHEL/CentOS 7.x Desktops

To set up True SSO for RHEL/CentOS 7.x desktops, first integrate the base virtual machine with an Active Directory domain. Then install the required libraries and root Certificate Authority (CA) certificate before installing Horizon Agent.

Integrate a RHEL/CentOS 7.x VM with AD for True SSO

To support True SSO on instant-cloned RHEL/CentOS 7.x desktops, you must configure Samba on the base virtual machine (VM).

The RHEL/CentOS 7.x `realmd` feature provides a simple way to discover and join identity domains. Instead of connecting the system to the domain itself, `realmd` configures underlying Linux system services, such as SSSD or Winbind, to connect to the domain. The following steps describe how to use `realmd` and Samba to perform an offline domain join of a RHEL/CentOS 7.x VM to Active Directory.

Prerequisites

Verify that:

- The RedHat Enterprise Linux (RHEL) system is subscribed to Red Hat Network (RHN) or has the `yum` tool installed locally.
- The Active Directory (AD) server is resolvable by DNS on the RHEL/CentOS 7.x VM.
- The Network Time Protocol (NTP) is configured on the VM.

Procedure

1 Verify that the RHEL/CentOS VM can discover the AD server. Use the following example, where *ADdomain.example.com* is replaced with your AD server information.

```
sudo realm discover ADdomain.example.com
```

2 Install the Samba `tdb-tools` package.

The Samba `tdb-tools` package is not available for download from the official Red Hat repository. You must download it manually. For example, use the following command to download it from a CentOS system and install the downloaded package on your RHEL system.

```
sudo yumdownloader tdb-tools
```

If you do not have a CentOS system, go to `https://rpmfind.net/linux/rpm2html/search.php?query=tdb-tools&submit=Search+...&system=&arch`, download the `tdb-tools-1.3.15-1.el7.x86_64.rpm` package, and install it on your RHEL system.

3 Install Samba and the dependency packages.

```
sudo yum install sssd-tools sssd adcli samba-common pam_ldap pam_krb5 samba samba-client
krb5-workstation
```

4 Run the `join` command, using the following example, where *DNSdomain.example.com* must be replaced with the DNS domain path specific for your environment.

```
sudo realm join DNSdomain.example.com -U administrator
```

When the join command succeeds, you receive the following message.

```
Successfully enrolled machine in realm
```

5 Restart the VM and log back in.

What to do next

Configure True SSO on a RHEL/CentOS 7.x VM

Configure True SSO on a RHEL/CentOS 7.x VM

To enable the True SSO feature on a RHEL/CentOS 7.x virtual machine (VM), install the libraries on which the True SSO feature depends, the root Certificate Authority (CA) certificate to support trusted authentication, and Horizon Agent. In addition, you must edit some configuration files to complete the authentication setup.

Use the following procedure to enable True SSO on a RHEL 7.x or CentOS 7.x VM.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the DNS name of your AD domain. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_server	Path to your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters

Prerequisites

- Configure True SSO for Workspace ONE Access and Horizon Connection Server.
- Complete the steps described in Integrate a RHEL/CentOS 7.x VM with AD for True SSO.

- Get a root Certificate Authority certificate and save it to `/tmp/certificate.cer` on your RHEL/CentOS 7.x VM. See How to Export Root Certification Authority Certificate.

  If a subordinate CA is also an issuing authority, then get the entire chain of root and subordinate CA certificates and save it to `/tmp/certificate.cer` on the VM.

Procedure

1 Install the PKCS11 support package group.

```
sudo yum install -y nss-tools nss-pam-ldapd pam_krb5 krb5-libs krb5-workstation krb5-pkinit
```

2 Install the root CA certificate or certificate chain.

a Locate the root CA certificate or certificate chain that you downloaded, and transfer it to a PEM file.

```
sudo openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

b Make an `/etc/pki/nssdb` directory to contain the system database.

```
sudo mkdir -p /etc/pki/nssdb
```

c Use the `certutil` command to install the root CA certificate or certificate chain to the system database `/etc/pki/nssdb`.

Replace "root CA cert" in the following example command with the name of the root CA certificate in the system database.

```
sudo certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/
certificate.pem
```

d Add the root CA certificate or certificate chain to the list of trusted CA certificates on the RHEL/CentOS 7.x VM and update the system-wide trust store configuration using the `update-ca-trust` command.

```
sudo cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
sudo update-ca-trust
```

3 Modify the appropriate section in your system's SSSD configuration file for your domain, as shown in the following example.

```
[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = MYDOMAIN.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
```

```
#set the next line to false, so you can use the short name instead of the full domain name.
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
```

4 Modify the Kerberos configuration file `/etc/krb5.conf`, as shown in the following example.

```
[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_ccache_name = KEYRING:persistent:%{uid}
 # Add following line, if the system doesn't add it automatically
 default_realm = MYDOMAIN.COM

[realms]
MYDOMAIN.COM = {
  kdc = dns_server
  admin_server = dns_server
  # Add the following three lines for pkinit_*
  pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
  pkinit_kdc_hostname = your_org_DNS_server
  pkinit_eku_checking = kpServerAuth
 }
[domain_realm]
 mydomain.com = MYDOMAIN.COM
 .mydomain.com = MYDOMAIN.COM
```

Note You must also set the mode equal to `644` in `/etc/krb5.conf`. Otherwise, the True SSO feature might not work.

5 Install the Horizon Agent package, with True SSO enabled.

```
sudo ./install_viewagent.sh -T yes
```

6 Add the following parameter to the Horizon Agent custom configuration file `/etc/vmware/viewagent-custom.conf`. Use the following example, where *NETBIOS_NAME_OF_DOMAIN* is the NetBIOS name of your organization's domain.

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

7 Restart the VM and log back in.

Configure True SSO with SSSD on Ubuntu/Debian Desktops

To enable True SSO on an Ubuntu/Debian desktop, integrate the base virtual machine (VM) with an Active Directory (AD) domain using the SSSD solution. Then install the root Certificate Authority (CA) certificate to support trusted authentication before installing Horizon Agent.

Use the following procedure to enable True SSO with SSSD on an Ubuntu/Debian VM.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the host name of your VM. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
myhost	Host name of your Ubuntu/Debian VM
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server
admin-user	User name of the AD domain administrator

Prerequisites

- Verify that the VM is running one of the following distributions.
  - Ubuntu 22.04/20.04
  - Debian 12.x/11.x

  Note True SSO with SSSD is not supported for Debian 10.x desktops. To configure True SSO on a Debian 10.x desktop, use Samba domain-join instead as described in Configure True SSO with Samba for Ubuntu/Debian Desktops.

- Configure True SSO for Workspace ONE Access and Horizon Connection Server.
- Get a root CA certificate and save it to `/tmp/certificate.cer` on the Ubuntu/Debian VM. See How to Export Root Certification Authority Certificate.

  If a subordinate CA is also an issuing authority, then get the entire chain of root and subordinate CA certificates and save it to `/tmp/certificate.cer` on the VM.

Procedure

1 On the base VM, verify the network connection to Active Directory.

```
sudo realm discover mydomain.com
```

2 Install the required dependency packages.

```
sudo apt-get install sssd-tools sssd libnss-sss libpam-sss adcli samba-common-bin krb5-
user krb5-pkinit
```

3 Join the AD domain.

```
sudo realm join --verbose mydomain.com -U admin-user
```

4 Install the root CA certificate or certificate chain.

a Locate the root CA certificate or certificate chain that you downloaded, and transfer it to a PEM file.

```
sudo openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

b Copy the certificate to the `/etc/sssd/pki/sssd_auth_ca_db.pem` file.

```
sudo cp /tmp/certificate.pem /etc/sssd/pki/sssd_auth_ca_db.pem
```

5 Modify the `/etc/sssd/sssd.conf` configuration file, as shown in the following example.

```
[sssd]
domains = mydomain.com
config_file_version = 2
services = nss, pam

[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = MYDOMAIN.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False #Use short name for user
fallback_homedir = /home/%u@%d
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred #Add this line for SSO
ad_gpo_access_control = permissive #Only add this line for Ubuntu 20.04 and Debian 12 to
fix https://bugs.launchpad.net/ubuntu/+source/sssd/+bug/1934997

[pam] #Add pam section for certificate login
pam_cert_auth = True #Add this line to enable certificate login for system
pam_p11_allowed_services = +gdm-vmwcred #Add this line to enable certificate login for
VMware Horizon Agent

[certmap/mydomain.com/truesso] #Add this section and following lines to set match and map
rule for certificate user
matchrule = <EKU>msScLogin
maprule = (|(userPrincipal={subject_principal})
(samAccountName={subject_principal.short_name}))
domains = mydomain.com
priority = 10
```

6. Change the access mode for the `/etc/krb5.conf` configuration file to make it editable.

   ```
   sudo chmod 644 /etc/krb5.conf
   ```

7. Modify the `/etc/krb5.conf` file, as shown in the following example.

   ```
   [realms]
    MYDOMAIN.COM = {
       kdc = kdcserver.mydomain.com
       admin_server = dnsserver.mydomain.com
       pkinit_anchors = DIR:/etc/sssd/pki
       pkinit_kdc_hostname = kdcserver.mydomain.com
       pkinit_eku_checking = kpServerAuth
    }

   [domain_realm]
       .mydomain.com = MYDOMAIN.COM
       mydomain.com = MYDOMAIN.COM
   ```

8. Install the Horizon Agent package, with True SSO enabled.

   ```
   sudo ./install_viewagent.sh -T yes
   ```

9. Modify the `/etc/vmware/viewagent-custom.conf` configuration file so that it includes the following line.

   ```
   NetbiosDomain = MYDOMAIN
   ```

10. Restart the VM and log back in.

Configure True SSO with Samba for Ubuntu/Debian Desktops

To set up True SSO for Ubuntu/Debian desktops, first integrate the base virtual machine with an Active Directory domain using the Samba and Winbind domain-join solutions. Then install the required libraries and root Certificate Authority (CA) certificate before installing Horizon Agent.

Note Alternatively, you can configure True SSO using the SSSD domain-join solution as described in Configure True SSO with SSSD on Ubuntu/Debian Desktops.

Domain-join an Ubuntu/Debian VM with Samba for True SSO

To support True SSO on Ubuntu/Debian desktops, you can integrate the base virtual machine (VM) with an Active Directory (AD) domain using the Samba and Winbind solutions.

Note Alternatively, you can configure True SSO using the SSSD domain-join solution as described in Configure True SSO with SSSD on Ubuntu/Debian Desktops.

To integrate an Ubuntu/Debian VM with an AD domain using Samba and Winbind, use the following procedure.

Some examples in the procedure use placeholder values to represent entities in your network configuration, such as the host name of your VM. Replace the placeholder values with information specific to your configuration, as described in the following table.

Placeholder Value	Description
dns_IP_ADDRESS	IP address of your DNS name server
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain, in all capital letters
myhost	Host name of your Ubuntu/Debian VM
MYDOMAIN	DNS name of the workgroup or NT domain that includes your Samba server, in all capital letters
ads-hostname	Host name of your AD server
admin-user	User name of the AD domain administrator

Prerequisites

Verify that:

- The AD server is resolvable by DNS on the VM.
- The Network Time Protocol (NTP) is configured on the VM.

Procedure

1 On the Ubuntu/Debian VM, install the `samba` and `winbind` packages.

```
sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
```

2 Configure the Kerberos Authentication settings.

a If the window for Kerberos Authentication settings does not appear on your system, run the following command to display it.

```
sudo dpkg-reconfigure krb5-config
```

b For **Default Kerberos version 5 realm**, enter the DNS name of your AD domain using all capital letters.

For example, if your AD domain name is **`mydomain.com`**, enter **`MYDOMAIN.COM`**.

c For **Kerberos servers for your realm**, enter the host name of your AD server (represented as **`ads_hostname`** in the examples throughout this procedure).

d For **Administrative server for your Kerberos realm**, enter the host name of your AD server again.

3 Update the PAM configuration.

   a Open the PAM configuration page.

   ```
   pam-auth-update
   ```

   b Select **Create home directory on login**, and then select **Ok**.

4 Edit the `/etc/nsswitch.conf` configuration file, as shown in the following example.

   ```
   passwd: compat winbind
   group: compat winbind
   shadow: compat
   gshadow: files
   ```

5 (Optional) If the system detects the correct DNS server automatically, skip this step and proceed to the next step. If the system fails to detect the correct DNS server, complete this step to set the DNS server manually.

   To ensure that the auto-generated `resolv.conf` file refers to your AD domain as a search domain, edit the NetworkManager settings for your system connection. The following substeps provide the example instructions for an Ubuntu 20.04 system.

   a Open the NetworkManager control panel and navigate to the **IPv4 Settings** for your system connection. For Method, select **Automatic (DHCP) addresses only**. In the **DNS servers** text box, enter the IP address of your DNS name server (represented as **`dns_IP_ADDRESS`** in the examples throughout this procedure). Then click **Save**.

   b Edit the `/etc/dhcp/dhclient.conf` file as shown in the following example.

   ```
   supersede domain-name "mydomain.com";
   prepend domain-name-servers dns_IP_ADDRESS;
   ```

   c Edit the `/etc/systemd/resolved.conf` file as shown in the following example.

   ```
   DNS=dns_IP_ADDRESS
   Domains="mydomain.com"
   ```

   Note A new virtual network adapter is added when a new instant-cloned virtual desktop is created. When you add the network adapter to a cloned virtual desktop, the virtual desktop template clears the settings for the network adapter, such as the DNS server. To keep the DNS server setting when adding a new network adapter, you must specify a DNS server for your VM.

d Specify the DNS server by editing the `/etc/resolv.conf` configuration file, as shown in the following example. If a warning appears, you can disregard and proceed with the changes.

```
nameserver dns_IP_ADDRESS

search mydomain.com
```

e Restart the VM and log back in.

6 Edit the `/etc/hosts` configuration file, as shown in the following example.

```
127.0.0.1     localhost
127.0.1.1     myhost.mydomain.com myhost
```

7 Edit the `/etc/samba/smb.conf` configuration file, as shown in the following example.

```
[global]
security = ads
realm = MYDOMAIN.COM
workgroup = MYDOMAIN
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
kerberos method = secrets and keytab
winbind refresh tickets = true
```

8 Restart the `smbd` service.

```
sudo systemctl restart smbd.service
```

9 Edit the `/etc/krb5.conf` configuration file so that it has content similar to the following example.

```
[libdefaults]
      default_realm = MYDOMAIN.COM
      dns_lookup_realm = true
      dns_lookup_kdc = true

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
      }
```

```
[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

10 Join the Ubuntu/Debian VM to the AD domain.

   a Initiate a Kerberos ticket.

   ```
    sudo kinit admin-user
   ```

   When prompted, enter your administrator password.

   b Verify that the ticket has been created successfully.

   ```
   sudo klist
   ```

   This command returns information about the ticket, including its valid starting time and expiration time.

   c Create a Kerberos keytab file.

   ```
   sudo net ads keytab create -U admin-user
   ```

   d Join the AD domain.

   ```
   sudo net ads join -U admin-user
   ```

11 Restart and verify the Winbind service.

   a Restart the Winbind service.

   ```
   sudo systemctl restart winbind.service
   ```

   b To verify the Winbind service, run the following commands and check that they return the correct output.

   - `sudo wbinfo -u`
   - `sudo wbinfo -g`
   - `sudo getent passwd`
   - `sudo getent group`

12 Restart the VM and log back in.

What to do next

Configure True SSO with Samba on Ubuntu/Debian Desktops

Configure True SSO with Samba on Ubuntu/Debian Desktops

To enable the True SSO feature on an Ubuntu/Debian virtual machine (VM), install the libraries on which the True SSO feature depends, the root Certificate Authority (CA) certificate to support trusted authentication, and Horizon Agent. If True SSO authentication is also issued by a subordinate CA, then you must install the entire certificate chain of root and subordinate CA certificates. To complete the authentication setup, you must edit some configuration files.

Note Alternatively, you can configure True SSO using the SSSD domain-join solution as described in Configure True SSO with SSSD on Ubuntu/Debian Desktops.

Use the following procedure to enable True SSO with Samba on an Ubuntu/Debian VM.

Prerequisites

- Configure True SSO for Workspace ONE Access and Horizon Connection Server.
- Complete the steps described in Domain-join an Ubuntu/Debian VM with Samba for True SSO .
- Get a root CA certificate and save it to `/tmp/certificate.cer` on the Ubuntu/Debian VM. See How to Export Root Certification Authority Certificate.

  If a subordinate CA is also an issuing authority, then get the entire chain of root and subordinate CA certificates and save it to `/tmp/certificate.cer` on the VM.

Procedure

1 On the VM, install the `pkcs11` support package.

```
sudo apt install libpam-pkcs11
```

2 Install the `libnss3-tools` package.

```
sudo apt install libnss3-tools
```

3 Install the root CA certificate or certificate chain.

a Locate the root CA certificate or certificate chain that you downloaded, and transfer it to a PEM file.

```
sudo openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

b Make an `/etc/pki/nssdb` directory to contain the system database.

```
sudo mkdir -p /etc/pki/nssdb
```

c Use the `certutil` command to install the root CA certificate or certificate chain to the system database `/etc/pki/nssdb`.

Replace "root CA cert" in the following example command with the name of the root CA certificate in the system database.

```
sudo certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/
certificate.pem
```

   d Make an /etc/pam_pkcs11/cacerts directory and copy the root CA certificate or certificate chain there.

   ```
   sudo mkdir -p /etc/pam_pkcs11/cacerts
   sudo cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
   ```

   e Create a hash link for the root CA certificate or certificate chain. In the /etc/pam_pkcs11/cacerts directory, run the following command.

   ```
   sudo pkcs11_make_hash_link
   ```

4 Install the Horizon Agent package, with True SSO enabled.

   ```
   sudo ./install_viewagent.sh -T yes
   ```

5 Add the following parameter to the Horizon Agent custom configuration file /etc/vmware/viewagent-custom.conf. Use the following example, where *NETBIOS_NAME_OF_DOMAIN* is the NetBIOS name of your organization's domain.

   ```
   NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
   ```

6 Edit the /etc/pam_pkcs11/pam_pkcs11.conf configuration file.

   a If needed, create the /etc/pam_pkcs11/pam_pkcs11.conf configuration file. Locate the example file in /usr/share/doc/libpam-pkcs11/examples, copy it to the /etc/pam_pkcs11 directory, and rename the file to pam_pkcs11.conf. Add your system information to the contents of the file as needed.

   b Modify the /etc/pam_pkcs11/pam_pkcs11.conf configuration file so that it includes content similar to the following example.

   Note For Ubuntu 20.04 or later, append ms to the end of the use_mappers line.

```
use_pkcs11_module = coolkey;
pkcs11_module coolkey {
  module = /usr/lib/vmware/viewagent/sso/libvmwpkcs11.so;
  slot_num = 0;
  ca_dir = /etc/pam_pkcs11/cacerts;
  nss_dir = /etc/pki/nssdb;
}

mapper ms {
  debug = false;
  module = internal;
  # module = /usr/$LIB/pam_pkcs11/ms_mapper.so;
  ignorecase = false;
  # ignore domain name
  ignoredomain = true;
  domain = "DOMAIN.COM"; #<== Replace "DOMAIN.COM" with your organization's domain name
}

use_mappers = digest, cn, pwent, uid, mail, subject, null, ms;  #<== For Ubuntu 20.04
or later, append "ms" at end of use_mappers
```

7 In the Linux terminal, set the access permissions for the /etc/krb5.conf configuration file to 644, as shown in the following example.

```
sudo chmod 644 /etc/krb5.conf
```

Verify that the permissions have been modified.

```
ls -l /etc/krb5.conf

-rw-r--r-- 1 root root xxx xx xx xxxx /etc/krb5.conf
```

Note If you do not modify the permissions of /etc/krb5.conf as specified, the True SSO feature might not work.

8 Restart the VM and log back in.

Configure True SSO for SLED/SLES Desktops

To set up True SSO for SLED/SLES desktops, first integrate the base virtual machine with an Active Directory domain. Then install the required libraries and root Certificate Authority (CA) certificate before installing Horizon Agent.

Integrate a SLED/SLES VM with AD for True SSO

To support True SSO on SLED/SLES desktops, first integrate the base virtual machine (VM) with an Active Directory (AD) domain using the Samba and Winbind solutions.

Use the following procedure to integrate a SLED/SLES VM with an AD domain.

Prerequisites

Verify the following:

- The True SSO feature has been configured for Workspace ONE Access and Horizon Connection Server.
- The SLED/SLES base VM meets the system requirements described in Set Up True SSO for Linux Desktops.
- The Active Directory server is resolvable by DNS on the VM.
- The Network Time Protocol (NTP) is configured on the VM.

Procedure

1 On the SLED/SLES VM, install the `samba` and `winbind` packages.

```
sudo zypper install samba-winbind krb5-client samba-winbind-32bit
```

2 Open the YaST setup tool and navigate to **Network Services > Windows Domain Membership**.

3 On the Windows Domain Membership screen, configure settings as follows.

   a For **Domain or Workgroup**, enter the DNS name of the workgroup or NT domain that includes your Samba server, using all capital letters. For example, if your workgroup name is **`mydomain`**, enter **`MYDOMAIN`**.

   b Select **Also Use SMB Information for Linux Authentication**.

   c Select **Create Home Directory on Login**.

   d Select **Offline Authentication**.

   e Select **Single Sign-on for SSH**.

4 At the prompt asking if you want to join the domain, select **Yes**.

5 Enter the administrator name and password for the specified workgroup, and select **OK**.

   A message appears confirming that the system joined the domain successfully. Select **OK**.

6 Edit the `/etc/samba/smb.conf` configuration file so that it includes the following parameter.

```
[global]
...
winbind use default domain = yes
```

7 Restart the VM and log back in.

8 Test and verify the AD integration.

   Run the following test commands and check that they return the correct output. Replace `mydomain` with the name of your Samba server workgroup or NT domain.

   - `sudo net ads testjoin`
   - `sudo net ads info`
   - `sudo wbinfo --krb5auth=mydomain\\open%open`
   - `sudo ssh localhost -l mydomain\\open`

What to do next

Proceed to Configure True SSO on a SLED/SLES VM.

Configure True SSO on a SLED/SLES VM

To enable the True SSO feature on a SLED/SLES virtual machine (VM), install the libraries on which the True SSO feature depends, the root Certificate Authority (CA) certificate to support trusted authentication, and Horizon Agent. In addition, you must edit some configuration files to complete the authentication setup.

Use the following procedure to enable True SSO on a SLED or SLES VM.

Prerequisites

- Configure True SSO for Workspace ONE Access and Horizon Connection Server.
- Complete the steps described in Integrate a SLED/SLES VM with AD for True SSO .
- Get a root Certificate Authority certificate and save it to `/tmp/certificate.cer` on your SLED/SLES VM. See How to Export Root Certification Authority Certificate.

  If a subordinate CA is also an issuing authority, then get the entire chain of root and subordinate CA certificates and save it to `/tmp/certificate.cer` on the VM.

Procedure

1 Install the required packages by running the following command.

```
sudo zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

2 Install the root CA certificate or certificate chain.

a Locate the root CA certificate or certificate chain that you downloaded, and transfer it to a PEM file.

```
sudo openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

b Make an `/etc/pki/nssdb` directory to contain the system database.

```
sudo mkdir -p /etc/pki/nssdb
```

c Use the `certutil` command to install the root CA certificate or certificate chain to the system database `/etc/pki/nssdb`.

Replace "root CA cert" in the following example command with the name of the root CA certificate in the system database.

```
sudo certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/
certificate.pem
```

d Add the root CA certificate to `pam_pkcs11`.

```
sudo cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
```

3 Edit the `/etc/krb5.conf` configuration file so that it has content similar to the following example.

```
[libdefaults]
      default_realm = MYDOMAIN.COM
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
            pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
            pkinit_kdc_hostname = ADS-HOSTNAME
            pkinit_eku_checking = kpServerAuth
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

Note You must also set the file permissions to `644` for `/etc/krb5.conf`. Otherwise, the True SSO feature might not work.

Replace the placeholder values in the example with information specific to your network configuration, as described in the following table.

Placeholder Value	Description
mydomain.com	DNS name of your AD domain
MYDOMAIN.COM	DNS name of your AD domain (in all capital letters)
ads-hostname	Host name of your AD server
ADS-HOSTNAME	Host name of your AD server (in all capital letters)

4. Install the Horizon Agent package, with True SSO enabled.

   ```
   sudo ./install_viewagent.sh -T yes
   ```

5. Add the following parameter to the Horizon Agent custom configuration file `/etc/vmware/viewagent-custom.conf`. Use the following syntax, where *NETBIOS_NAME_OF_DOMAIN* is the name of your organization's NetBIOS domain.

   ```
   NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
   ```

   Note Always use the long name of the NetBIOS domain, for example `LXD.VDI`. If you use the short name, such as `LXD`, the True SSO feature does not work.

6. Restart the VM and log back in.

Setting Up Graphics for Linux Virtual Machines

5

This page describes the graphics capabilities of Linux virtual machines (VMs) that serve as sources for VMware Horizon 8 desktop pools. You can configure the currently supported Linux distributions to take advantage of NVIDIA virtual shared pass-through graphics acceleration (vGPU) capabilities on the ESXi host.

Note The information on this page and its sub-pages is applicable only to Linux VMs. For information about graphics requirements and capabilities for physical Linux machines, see Prepare a Physical Linux Machine for Desktop Deployment.

Horizon Agent only supports vGPU capabilities for Linux VMs, and does not support virtual dedicated graphics acceleration (vDGA).

Note For information about the NVIDIA graphics cards and Linux distributions that support vGPU capabilities, see https://docs.nvidia.com/grid/latest/product-support-matrix/index.html.

Keep in mind the following points when configuring a Linux desktop to support vGPU capabilities:

Caution Before you begin, verify that Horizon Agent is not installed on the Linux virtual machine. If you install Horizon Agent before you configure the machine to use NVIDIA vGPU, required configuration parameters in the `xorg.conf` file are overwritten, and NVIDIA vGPU does not work. You must install Horizon Agent after the NVIDIA vGPU configuration is completed.

- You must use the NVIDIA Linux VM display driver that matches the ESXi host GPU driver (`.vib`). See the NVIDIA website for information about driver packages.
- To support vGPU capabilities on cloned VMs, first complete the graphics setup in the base VM and then clone the VMs. The graphics settings work for cloned VMs and no further settings are required.

Read the following topics next:

- Install the VIB for the NVIDIA GRID vGPU Graphics Card on the ESXi Host
- Configure a Shared PCI Device for vGPU on the Linux VM
- Install the NVIDIA GRID vGPU Display Driver on a Linux VM
- Verify the NVIDIA Display Driver on a Linux VM

Install the VIB for the NVIDIA GRID vGPU Graphics Card on the ESXi Host

To support vGPU capabilities on a Linux desktop, you must download and install the VIB for your NVIDIA GRID graphics card on the ESXi host.

NVIDIA provides a vGPU software package that includes a vGPU Manager, which you install on the ESXi host in this procedure, and a Linux Display Driver, which you can install on the Linux virtual machine in a later procedure.

Prerequisites

- Verify that vSphere 7 U3 or a later release is installed in your environment.

  Note To support vGPU capabilities on Linux application pools, you must use vSphere 7 U3 or later.

- Verify that the required vGPU graphics card is installed on the ESXi host.

Note For information about the NVIDIA graphics cards and Linux distributions that support vGPU capabilities, see https://docs.nvidia.com/grid/latest/product-support-matrix/index.html.

Procedure

1 Download the VIB for your NVIDIA GRID vGPU graphics card from the NVIDIA website.

  Select the appropriate VIB version from the drop-down menus.

Option	Description
Product Type	**GRID**
Product Series	Select **NVIDIA GRID vGPU**.
Product	Select the version (such as **GRID K2**) that is installed on the ESXi host.
Operating System	Select the VMware vSphere ESXi version.

2 Uncompress the vGPU software package `.zip` file.

3 Upload the vGPU Manager folder to the ESXi host.

  Note You can install the Linux Display Driver on the Linux virtual machine in a later procedure.

4 Power off or suspend all virtual machines on the ESXi host.

5 Connect to the ESXi host using SSH.

6 Stop the `xorg` service.

```
# /etc/init.d/xorg stop
```

7 Install the NVIDIA VIB.

For example:

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```

8 Reboot or update the ESXi host.

- For an installed ESXi host, reboot the host.
- For a stateless ESXI host, take the following steps to update the host. (These steps also work on an installed host.)

```
Update vmkdevmgr:
# kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)

Wait for the update to complete:
# localcli --plugin-dir /usr/lib/vmware/esxcli/int deviceInternal bind

This is a new requirement with the NVIDIA 352.* host driver:
# /etc/init.d/nvidia-vgpu start

Restart xorg, which is used for GPU assignment:
# /etc/init.d/xorg start
```

9 Verify that the `xorg` service is running after the host restart.

Configure a Shared PCI Device for vGPU on the Linux VM

To use NVIDIA vGPU, you must configure a shared PCI device for the Linux virtual machine (VM).

Prerequisites

- Verify that the Linux virtual machine is prepared for use as a desktop. See Create a Virtual Machine and Install Linux and Prepare a Linux Machine for Remote Desktop Deployment.
- Verify that Horizon Agent is not installed on the Linux virtual machine.
- Verify that the NVIDIA VIB is installed on the ESXi host. See Install the VIB for the NVIDIA GRID vGPU Graphics Card on the ESXi Host.
- Familiarize yourself with the virtual GPU types that are available with NVIDIA vGPU, which you select with the **GPU Profile** setting. The virtual GPU types provide varying capabilities on the physical GPUs installed on the ESXi host.

Note For information about the NVIDIA graphics cards and Linux distributions that support vGPU capabilities, see https://docs.nvidia.com/grid/latest/product-support-matrix/index.html.

Procedure

1 Power off the virtual machine.

2 In vSphere Client, select the virtual machine and, under the **VM Hardware** tab, click **Edit Settings**.

3 In the **New device** menu, select **Shared PCI Device**.

4 Click **Add** and select **NVIDIA GRID vGPU** from the drop-down menu.

5 For the **GPU Profile** setting, select a virtual GPU type from the drop-down menu.

> **Note** To support vGPU capabilities on Linux application pools, you must select the profile that assigns the full memory of the physical GPU to the VM. This means selecting the highest available vGPU profile from the list of options.

6 Click **Reserve all memory** and click **OK**.

You must reserve all virtual machine memory to enable the GPU to support NVIDIA GRID vGPU.

7 Power on the virtual machine.

Install the NVIDIA GRID vGPU Display Driver on a Linux VM

To install the NVIDIA GRID vGPU display driver, you must deactivate the default NVIDIA driver, download the NVIDIA display drivers, and configure the PCI device on the Linux virtual machine (VM).

Prerequisites

- Verify that you downloaded the vGPU software package from the NVIDIA download site, uncompressed the package, and have the Linux Display Driver (a package component) ready. See Install the VIB for the NVIDIA GRID vGPU Graphics Card on the ESXi Host.

  Also verify that a shared PCI device was added to the virtual machine. See Configure a Shared PCI Device for vGPU on the Linux VM .

Procedure

1 Copy the NVIDIA Linux Display Driver to the virtual machine.

2 Open a remote terminal to the virtual machine, or switch to a text console by typing Ctrl-Alt-F2, log in as root, and run the `init 3` command to turn off X Windows.

3 Install additional components that are required for the NVIDIA driver.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

4 Add an executable flag to the NVIDIA GRID vGPU driver package.

```
chmod +x NVIDIA-Linux-x86_64-version-grid.run
```

5. Start the NVIDIA GRID vGPU installer.

   ```
   sudo ./NVIDIA-Linux-x86_64-version-grid.run
   ```

6. Accept the NVIDIA software license agreement and select **Yes** to update the X configuration settings automatically.

What to do next

Install Horizon Agent on the Linux virtual machine. See Install Horizon Agent on a Linux Machine.

Verify the NVIDIA Display Driver on a Linux VM

You can verify that the NVIDIA display driver is installed on a Linux virtual machine (VM) by displaying the NVIDIA driver output in a desktop session.

Prerequisites

- Verify that you installed the NVIDIA display driver.
- Verify that Horizon Agent is installed on the Linux virtual machine. See Install Horizon Agent on a Linux Machine.
- Verify that the Linux virtual machine is deployed in a desktop pool.

Procedure

1. Restart the Linux virtual machine.

   The Horizon Agent startup script initializes the X server and display topology.

   You can no longer view the virtual machine display in the vSphere console.

2. From Horizon Client, connect to the Linux desktop.
3. In the Linux desktop session, verify that the NVIDIA display driver is installed.

   Open a terminal window and run the `glxinfo | grep NVIDIA` command.

   The NVIDIA driver output is displayed. For example:

   ```
   [root]# glxinfo | grep NVIDIA
   server glx vendor string: NVIDIA Corporation
   client glx vendor string: NVIDIA Corporation
   OpenGL vendor string: NVIDIA Corporation
   OpenGL version string: 4.5.0 NVIDIA 346.47
   OpenGL shading language version string: 4.50 NVIDIA
   ```

Results

The user can access the NVIDIA graphics capabilities on the remote desktop.

After verifying the installation of NVIDIA display driver, perform the following tasks for installation to work correctly.

- If you upgrade the Linux kernel, Horizon Agent might not communicate with Horizon Connection Server. To resolve the problem, reinstall the NVIDIA driver.
- Set the NVIDIA GRID licensing in the Linux VM. See the NVIDIA documentation for more information. If licensing is not set, the Linux desktop does not work correctly. For example, auto-fit does not work.

Configuration Options for Linux Desktops

6

You can configure various options to customize the user experience using configuration files.

Read the following topics next:

Edit Configuration Files on a Linux Desktop

For Linux desktops, you can configure certain options by editing entries in the `/etc/vmware/config` file, `/etc/vmware/viewagent-custom.conf` file, and `/etc/vmware/viewagent-greeter.conf` file.

During Horizon Agent installation, the installer copies the following configuration template files to `/etc/vmware`:

- `config.template`
- `viewagent-custom.conf.template`
- `viewagent-greeter.conf.template`

In addition, if `/etc/vmware/config`, `/etc/vmware/viewagent-custom.conf`, and `/etc/vmware/viewagent-greeter.conf` do not exist, the installer performs the following actions:

- Copies `config.template` to `config`
- Copies `viewagent-custom.conf.template` to `viewagent-custom.conf`
- Copies `viewagent-greeter.conf.template` to `/etc/vmware/viewagent-greeter.conf`

The configuration files list and document all the Horizon Agent for Linux configuration options. To set an option, remove the comment and change the value, as appropriate.

For example, the following line in /etc/vmware/config enables the build to lossless PNG mode.

```
RemoteDisplay.buildToLossless=TRUE
```

After you make configuration changes, reboot Linux to make the changes take effect.

Configuration Options in /etc/vmware/config

The VMware BlastServer and BlastProxy processes, along with their related plug-ins and processes, use the /etc/vmware/config configuration file.

Note The following table includes descriptions of each agent-enforced policy setting for USB devices in the Horizon Agent configuration file. Horizon Agent uses these settings Horizon Agent also passes these settings to Horizon Client for interpretation and enforcement. The enforcement depends on whether you specify the merge (**(m)**) modifier to apply the Horizon Agent filter policy setting in addition to the Horizon Client filter policy setting, or override the **(o)** modifier to use the Horizon Agent filter policy setting instead of the Horizon Client filter policy setting.

Table 6-1. Configuration Options in /etc/vmware/config

	Value/Format	Default	Description
appScanner.logLevel	error, warn, info, or debug	info	Use this option to specify the level of detail reported in the appScanner log file, which records activity related to remote application sessions. Valid values range from the least detailed "error" level to the most detailed "debug" level. You can find the appScanner log at /tmp/vmware-root/vmware-appScanner-<pid>.log, where <pid> is the ID of the appScanner process.
Option	error, warn, info, verbose, debug, or trace	info	Use this option to specify the level of detail reported in the BlastProxy log file. Valid values range from the least detailed "error" level to the most detailed "trace" level. You can find the BlastProxy log at /tmp/vmware-root/vmware-BlastProxy-<pid>.log, where <pid> is the ID of the BlastProxy process.
BlastProxy.UdpEnabled	true or false	true	Use this option to specify whether BlastProxy forwards UDP requests through secured port 22443 to Horizon Agent. true enables UDP forwarding. false deactivates UDP forwarding.
cdrserver.cacheEnable	true or false	true	Set this option to enable or deactivate the write caching feature from the agent towards the client side.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
cdrserver.customizedSharedFolderPath	`folder_path`	`/home/`	Use this option to change the client drive redirection shared folder location from the default `/home/`*`user`*`/tsclient` directory to a custom directory. For example, if the user `test` wants to place the client drive redirection shared folder at `/mnt/test/tsclient` instead of `/home/test/tsclient`, the user can specify **`cdrserver.customizedSharedFolderPath=/mnt/`**. **Note** For this option to take effect, the specified folder must exist and be configured with the correct user permissions.
cdrserver.forcedByAdmin	`true` or `false`	`false`	Set this option to control whether the client can share folders that you have not specified with the `cdrserver.shareFolders` option.
cdrserver.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the `vmware-CDRserver.log` file.
cdrserver.permissions	`R`	`RW`	Use this option to apply read/write permissions that Horizon Agent has on the folders shared by Horizon Client. For example: ■ If the folder shared by Horizon Client has `read` and `write` permissions and you set **`cdrserver.permissions=R`**, then Horizon Agent has only `read` access permissions. ■ If the folder shared by Horizon Client has only `read` permissions and you set **`cdrserver.permissions=RW`**, Horizon Agent still has only `read` access rights. Horizon Agent cannot change the `read` only attribute set by Horizon Client. Horizon Agent can only remove the write access rights. Typical uses are as follows: ■ **`cdrserver.permissions=R`** ■ **`#cdrserver.permissions=R`** (for example, comment it out or delete the entry)

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
cdrserver.sharedFolders	***file_path1*,R;*file-path2*,;** ***file_path3*,R; ...**	undefined	Specify one or more file paths to the folders that the client can share with the Linux desktop. For example: - For a Windows client: **`C:\spreadsheets,;D:\ebooks,R`** - For a non-Windows client: **`/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R`**
Clipboard.Direction	`0`, `1`, `2`, or `3`	`2`	Use this option to specify the clipboard redirection policy. Valid values are as follows: - 0 - Deactivate clipboard redirection. - 1 - Enable clipboard redirection in both directions. - 2 - Enable clipboard redirection from the client to the remote desktop only. - 3 - Enable clipboard redirection from the remote desktop to the client only.
collaboration.enableControlPassing	`true` or `false`	`true`	Set this option to permit or restrict collaborators from having control of the Linux desktop. To specify a read-only collaboration session, set this option to **`false`**.
collaboration.enableEmail	`true` or `false`	`true`	Set this option to enable or deactivate sending of collaboration invitations by using an installed email application. When this option is deactivated, you cannot use email to invite collaborators, even if you have installed an email application.
collaboration.logLevel	`error`, `info`, or `debug`	`info`	Use this option to set the log level used for the collaboration session. If the log level is `debug`, all calls made to `collabui` functions and the contents of the `collabor` list are logged.
collaboration.maxCollabors	An integer less than or equal to 20	5	Specifies the maximum number of collaborators that you can invite to join a session.
collaboration.serverUrl	[URL]	undefined	Specifies the server URLs to include in the collaboration invitations.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
Desktop.displayNumberMax	An integer	`159`	Specifies the upper limit of the range of X Window System display numbers to allocate to user sessions. This feature is not supported on SLED/SLES desktops. To restrict the allocation to a single display number, set `Desktop.displayNumberMax` and `Desktop.displayNumberMin` to the same value. **Note** If you specify a range that includes any of the display numbers 0 through 9, a conflict might occur with X server. Use the workaround described in VMware Knowledge Base (KB) article 81704.
Desktop.displayNumberMin	An integer	`100`	Specifies the lower limit of the range of X Window System display numbers to allocate to user sessions. This feature is not supported on SLED/SLES desktops. To restrict the allocation to a single display number, set `Desktop.displayNumberMax` and `Desktop.displayNumberMin` to the same value. **Note** If you specify a range that includes any of the display numbers 0 through 9, a conflict might occur with X server. Use the workaround described in VMware Knowledge Base (KB) article 81704.
DesktopWorker.ttyNum	An integer from 2 through 12	`7`	Assigns the TTY function key to display the graphical desktop on a physical Linux host machine. The default value is `7`, which assigns Ctrl+Alt+F7 as the shortcut to display the graphical desktop. This option applies to physical host machines only.
mksVNCServer.useUInputButtonMapping	`true` or `false`	`false`	Set this option to enable the support of a left-handed mouse on Ubuntu and SLED/SLES desktops, and on RHEL desktops running MATE. For more information, see VMware Knowledge Base (KB) article 90098.
mksvhan.clipboardSize	An integer	1024	Use this option to specify the clipboard maximum size to copy and paste.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
pcscd.maxReaderContext	An integer	Uses the value defined by the PC/SC Smart Card Daemon (pcscd)	Specifies the maximum number of reader contexts, or slots, allowed for smart card redirection. Use this option to ensure that the maximum number of reader contexts matches the value specified by your custom PC/SC Lite library.
pcscd.readBody	`true` or `false`	Uses the value defined by the PC/SC Smart Card Daemon (pcscd)	Specifies whether or not to read the body of `wait_reader_state_change` in the `CMD_WAIT_READER_STATE_CHANGE` or `CMD_STOP_WAITING_READER_STATE_CHANGE` PC/SC Lite message handler. Specify `true` to read the message body. Specify `false` to skip reading the message body. Use this option to ensure that the message reading setting of the smart card redirection feature matches the setting specified by your custom PC/SC Lite library. This option only takes effect when the `pcscd.maxReaderContext` is configured.
printSvc.customizedPpd	***`printer_name_1=ppd_path_1;printer_name_2=ppd_path_2...`***	undefined	Use this option to specify the file paths to custom PPD files for printers redirected through VMware Integrated Printing. You must define the custom PPD file path for every printer that does not use a Native Printer Driver (NPD) or Universal Printer Driver (UPD). Enter the printer name as defined on the client system and enter the absolute file path to the custom PPD file on the agent machine. Use semicolons between entries in the list.

Table 6-1. Configuration Options in /etc/vmware/config (continued)

	Value/Format	Default	Description

printSvc.defaultPrintOptions	List of space-separated print settings:
	ColorMode= Color or Mono
	Duplex= None, DuplexTumble, or DuplexNoTumble
	PageSize= string representing the media size
	number-up= an integer
	number-up-layout= None, lrtb, lrbt, rltb, rlbt, tblr, tbrl, btlr, or btrl
	OutputOrder= Normal or Reverse
	page-set= all, even, or odd
	noCollate or Collate
		ColorMode=Color
		Duplex=None
		PageSize=A4
		number-up=1
		number-up-layout=None
		OutputOrder=Normal
		page-set=all
		noCollate
			Use this option to specify the default print settings used to print output through VMware Integrated Printing if the source application cannot detect print settings. Enter the case-sensitive values and use spaces between entries in the list.
			Note This option is supported only when printing from Horizon Client for Windows, Horizon Client for Linux, or Horizon Client for Mac.
			■ ColorMode specifies whether to print in color or grayscale (Mono).
			■ Duplex specifies whether to print on one side of the sheet only (None), both sides with short-edge flip (DuplexTumble), or both sides with long-edge flip (DuplexNoTumble.
			■ PageSize specifies the page dimensions of the paper sheet. For the allowed values, refer to the registered mediaOption keywords listed in the Adobe PostScript Printer Description File Format Specification.
			■ number-up specifies the number of pages to arrange on a sheet in an imposition layout.
			■ number-up-layout specifies the arrangement to use in the imposition layout. For example, if number-up=4 and number-up-layout=lrtb, page 1 is placed at the top left, page 2 at the top right, page 3 at the bottom left, and page 4 at the bottom right corner of the sheet.
			■ OutputOrder specifies whether to print starting from the first page and ending with the last page (Normal) or starting from the last page and ending with the first page (Reverse).
			■ page-set specifies whether to print all pages, only the even-numbered pages, or only the odd-numbered pages.
			■ noCollate/Collate specifies whether or not to collate pages in a multiple-copy print job.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
printSvc.enable	`true` or `false`	`true`	Enables or deactivates the VMware Integrated Printing feature, which includes client printer redirection. **Note** To enable VMware Integrated Printing, you must set **both** of these configuration options to `true`: ■ `printSvc.enable` in `/etc/vmware/config` ■ `PrintRedirEnable` in `/etc/vmware/viewagent-custom.conf` If you set either one of these options to `false`, even with the other option set to `true`, VMware Integrated Printing is deactivated.
printSvc.jobOwnerAsLocal	`true` or `false`	`false`	Defines which user name to set as the print job owner name for the VMware Integrated Printing feature. Specify `true` to set the local user name as the print job owner name. Specify `false` to set the name used to log in to the remote session as the print job owner name.
printSvc.logLevel	`error`, `warn`, `info`, or `debug`	`info`	Sets the log level for the VMware Integrated Printing event log.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description

printSvc.paperListFile	File path to a configuration file containing the list of available paper sizes for printing	undefined	Use this option to define the list of paper sizes that can be used for printing output through VMware Integrated Printing. When you specify the path to a properly formatted configuration file, only those paper sizes listed in the configuration file are available as options when printing.
			Note This option is supported only when printing from Horizon Client for Windows. This option applies globally to all redirected printers on a Windows client system.
			You must follow these formatting rules when creating the configuration file.
			■ Each line in the configuration file corresponds to a specific paper size definition and must follow this format: **keyword, name, widthMm*10, heightMm*10, widthPts, heightPts**
			■ **keyword**: Enter a unique string that identifies the paper size. The keyword has a maximum length of 40 characters and can contain only printable ASCII characters within the range of decimal 33 to decimal 126, inclusive. For guidelines on industry-standard keyword strings, see the registered mediaOption keywords listed in the Adobe PostScript Printer Description File Format Specification.
			■ **name**: Specify the display name of the paper size as you want it to appear in the application print settings.
			■ **widthMm*10**: Enter the width of the paper in millimeters, multiplied by 10.
			■ **heightMm*10**: Enter the height of the paper in millimeters, multiplied by 10.
			■ **widthPts**: Enter the width of the paper in points.
			■ **heightPts**: Enter the height of the paper in points.
			Refer to the following example of a properly formatted configuration file:
			`Letter, Letter, 2159, 2794, 612, 792`
			`A3, A3, 2970, 4200, 842, 1191`
			`A4, A4, 2100, 2970, 595, 842`

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
printSvc.printerFilter	Logical combination of one or more search queries	undefined	Use this option to define a filter that specifies the client printers to exclude from VMware Integrated Printing redirection. Printers specified in the filter are not redirected and do not appear as available printers on the Linux desktop. Follow these guidelines when defining the printer filter. ■ You can construct search queries based on the printer name (**PrinterName**), driver name (**DriverName**), or driver vendor name (**DriverVendorName**). ■ Regular expressions and wildcards are supported. ■ To specify a range of characters, use square brackets **[ ]**, for example, `[a-z]`. ■ To specify wildcards, use **.*** or **.?** ■ The following logical operators are supported: ■ **=** ■ **AND** ■ **OR** ■ **NOT** and **!=** ■ Enclose individual match expressions within single quotation marks. ■ Enclose the entire search query within double quotation marks. For example, the following filter excludes all printers whose printer name includes the string 'Port' or 'DFCreator' preceded by wildcard characters, and whose driver name includes the string 'Acme'. `printSvc.printerFilter="(PrinterName='Port' OR PrinterName='.?DFCreator') AND DriverName='Acme'"`
printSvc.usePdfFilter	`true` or `false`	`true`	Updates or does not update the PPD files of redirected printers to use PDF as the print format. **Note** This option is supported only when printing from Horizon Client for Linux or Horizon Client for Mac. This option applies globally to all redirected printers on a Linux or Mac client system.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
printSvc.watermarkEnabled	`true` or `false`	`false`	Set this option to enable or deactivate the ability to include a watermark with jobs printed using VMware Integrated Printing. For more information, see Add Watermarks With VMware Integrated Printing on Linux Desktops.
rdeSvc.allowDisplayScaling	`true` or `false`	`false`	Set this option to enable or deactivate display scaling, which changes the size of text, icons, and navigation elements.
rdeSvc.blockedWindows	List of semicolon-separated paths to application executables	N/A	Use this option to block specific applications from starting as a remote application session. Specify the path to each application executable and use semicolons to separate entries in the list. For example: **`rdeSvc.blockedWindows=/usr/libexec/gnome-terminal-server;`**
rdeSvc.enableOptimizedResize	`true` or `false`	`true`	Set this option to enable or deactivate optimized window resizing for published application sessions in Horizon Client for Windows. When this option is enabled, Windows client users can resize published application windows without encountering screen artifacts.
rdeSvc.enableWatermark	`true` or `false`	`false`	Enables or deactivates the digital watermark feature. For information about the feature, see Features of Linux Desktops in VMware Horizon 8.
rdeSvc.watermark.fit	`0`: Tile `1`: Center `2`: Multiple	`0`	Defines the layout of the digital watermark on the screen, which is divided into nine squares: ■ 0 = Tile: Watermark appears in all nine squares. Application sessions always use this layout. ■ 1 = Center: Watermark appears in the center square. ■ 2 = Multiple: Watermark appears in the center and four corner squares. If the watermark size exceeds the square size, it is scaled to maintain the aspect ratio.

rdeSvc.watermark.font	`serif`
	`sans-serif`
	`cursive`
	`fantasy`
	`monospace`
		`serif`	Defines the font used for the digital watermark.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
rdeSvc.watermark.fontSize	An integer within the range of values: `8-72`	`12`	Defines the font size (in points) of the digital watermark.
rdeSvc.watermark.margin	An integer within the range of values: `0-1024`	`50`	Defines the amount of space (in pixels) around the digital watermark for the Tile layout. As the watermark scales, the margin also scales proportionally.
rdeSvc.watermark.opacity	An integer within the range of values: `0-255`	`50`	Defines the transparency level of the digital watermark text.
rdeSvc.watermark.rotation	An integer within the range of values: `0-360`	`45`	Defines the display angle of the digital watermark text.

rdeSvc.watermark.template	String constructed using any of the available information variables:
	`$BROKER_USER_NAME`
	`$BROKER_DOMAIN_NAME`
	`$USER_NAME`
	`$USER_DOMAIN`
	`$MACHINE_NAME`
	`$REMOTE_CLIENT_IP`
	`$CLIENT_CONNECT_TIME`
		`$USER_DOMAIN\`
		`$USER_NAME\n`
		`$MACHINE_NAME`
		`On`
		`$CLIENT_CONNECT_TIME`
		`\n$REMOTE_CLIENT_IP`
			Defines the text that you want to display for the digital watermark. Construct the watermark using any combination and order of the information variables. The character limit is 1024 characters and 4096 characters after expansion. The text is truncated if it exceeds the maximum length.

RemoteDisplay.allowAudio	`true` or `false`	`true`	Set this option to enable or deactivate audio out.
RemoteDisplay.allowH264	`true` or `false`	`true`	Set this option to enable or deactivate H.264 encoding.
RemoteDisplay.allowH264YUV444	`true` or `false`	`true`	Set this option to enable or deactivate H.264 YUV 4:4:4 encoding with High Color Accuracy if the client supports it.
RemoteDisplay.allowHEVC	`true` or `false`	`true`	Set this option to enable or deactivate High Efficiency Video Coding (HEVC).
RemoteDisplay.allowHEVCYUV444	`true` or `false`	`true`	Set this option to enable or deactivate HEVC YUV 4:4:4 with High Color Accuracy if the client supports it.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
RemoteDisplay.allowVMWKeyEvent2Unicode	`true` or `false`	`true`	Set this option to allow or not allow Horizon Agent to process Unicode events representing keyboard input from clients. When this option is enabled, client systems send Unicode values representing keyboard input to the remote desktop. Since Linux does not support Unicode input natively, Horizon Agent first converts the Unicode values to KeyCodes and then sends the KeyCodes to the operating system to display the appropriate Unicode characters. When this option is deactivated, Horizon Agent does not handle any Unicode events sent from clients.
RemoteDisplay.buildToLossless	`true` or `false`	`false`	Graphic applications, especially graphic design applications, require pixel-exact rendering of images in the client display of a Linux desktop. You can configure the build-to-lossless mode for images and video playback that are generated on a Linux desktop and rendered on the client device. This feature uses additional bandwidth between the client and the ESXi host. Enabling this option deactivates the H.264 encoding.
RemoteDisplay.cursorWarpingMaxDelayMsec	An integer >= 250	1000	This setting tunes mouse cursor warping detection. It represents the longest delay since the user's latest mouse interaction that agent-side mouse movement will be tested for being a cursor warp. Higher values improve the accuracy of warp detection and prevent contention between the agent and client mouse movement. Lower values improve the speed of detection of mouse movement that does not originate from Horizon Client, such as mouse movements made by the remote user during screen sharing with Zoom or Microsoft Teams.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
RemoteDisplay.cursorWarpingSimulateUserInput	`true` or `false`	`false`	This setting works around limitations in applications that do not support cursor warping, such as Microsoft Teams' and Zoom's screen sharing feature. If set to `true`, when Horizon Agent detects mouse cursor warping, such as sudden mouse movement originating from Horizon Agent rather than Horizon Client, it will simulate this mouse motion as if coming from Horizon Client. This is useful if a user is sharing their Horizon Agent desktop screen using Microsoft Teams or Zoom and wants cursor warping to be seen by users with whom they are sharing the screen.
RemoteDisplay.enableCursorWarping	`true` or `false`	`false`	Set this option to `true` to activate the cursor warping detection feature. When the setting is activated, the remote agent detects sudden mouse position changes initiated on the agent and reflects them to the client by moving the user's local mouse cursor. When the setting is deactivated, the client ignores sudden cursor movements in the remote agent. This setting is deactivated by default (set to `false`).
RemoteDisplay.enableNetworkContinuity	`true` or `false`	`true`	Set this option to enable or deactivate the Network Continuity feature in Horizon Agent for Linux.
RemoteDisplay.enableNetworkIntelligence	`true` or `false`	`true`	Set this option to enable or deactivate the Network Intelligence feature in Horizon Agent for Linux.
RemoteDisplay.enableStats	`true` or `false`	`false`	Enables or deactivates the VMware Blast display protocol statistics in mks log, such as bandwidth, FPS, RTT, and so on.
RemoteDisplay.enableUDP	`true` or `false`	`true`	Set this option to enable or deactivate UDP protocol support in Horizon Agent for Linux.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
RemoteDisplay.maxBandwidthBurstMsec	An integer	1000	Specifies the bandwidth bursting interval for data sent to clients. This option configures the interval of time, in milliseconds, during which the network bandwidth can temporarily exceed the bandwidth cap set by `RemoteDisplay.maxBandwidthKbps`. For example, if `RemoteDisplay.maxBandwidthKbps` = 4000 and `RemoteDisplay.maxBandwidthBurstMsec` = 1000, then during a one-second interval the output must not exceed 4 Kbits. However, these 4 Kbits of data can be output as a concentrated burst at the start of the one-second interval or distributed throughout the one-second interval, as needed.
RemoteDisplay.maxBandwidthKbps	An integer	1000000	Specifies the maximum bandwidth in kilobits per second (Kbps) for a VMware Blast session. The bandwidth includes all imaging, audio, virtual channel, and VMware Blast control traffic. Valid value must be less than 4 Gbps (4096000). **Note** The maximum bandwidth actually allowed is the **lesser** of the following values: ■ The maximum bandwidth configured explicitly in `RemoteDisplay.maxBandwidthKbps` ■ The maximum bandwidth cap calculated from `RemoteDisplay.maxBandwidthKbpsPerMegaPixelOffset` and `RemoteDisplay.maxBandwidthKbpsPerMegaPixelSlope`
RemoteDisplay.maxBandwidthKbpsPerMegaPixelOffset	An integer	0	Specifies the offset and slope values used to determine the maximum bandwidth cap, in kilobits per second (Kbps), for a VMware Blast session, based on the total screen area available for the session. This maximum bandwidth cap is calculated from the equation `MaxBandwidthCap = Offset + (Slope * ScreenArea)`

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
RemoteDisplay.maxBandwidthKbpsPerMegaPixelSlope	An integer from 100 through 100000	6200	where ■ `Offset` is the value, in Kbps, defined by `RemoteDisplay.maxBandwidthKbpsPerMegaPixelOffset` ■ `Slope` is the value, in Kbps per megapixel, defined by `RemoteDisplay.maxBandwidthKbpsPerMegaPixelSlope` ■ `ScreenArea` is the total available screen area, in megapixels, of the monitors used to display the Blast session. This megapixel screen area is detected automatically during the session. **Note** The maximum bandwidth actually allowed is the **lesser** of the following values: ■ The maximum bandwidth configured explicitly in `RemoteDisplay.maxBandwidthKbps` ■ The maximum bandwidth cap calculated from `RemoteDisplay.maxBandwidthKbpsPerMegaPixelOffset` and `RemoteDisplay.maxBandwidthKbpsPerMegaPixelSlope`
RemoteDisplay.minBandwidthKbps	An integer	256	Specifies the minimum bandwidth in kilobits per second (Kbps) for a VMware Blast session. The bandwidth includes all imaging, audio, virtual channel, and VMware Blast control traffic.
RemoteDisplay.maxFPS	An integer	30	Specifies the maximum rate of screen updates. Use this setting to manage the average bandwidth that users consume. Valid value must be from 3 through 60. The default is 30 updates per second.
RemoteDisplay.maxQualityJPEG	available range of values: 1–100	90	Specifies the image quality of the desktop display for JPEG/PNG encoding. The high-quality settings are for areas of the screen that are more static, resulting in a better image quality.
RemoteDisplay.midQualityJPEG	available range of values: 1–100	35	Specifies the image quality of the desktop display for JPEG/PNG encoding. Use to set the medium-quality settings of the desktop display.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
RemoteDisplay.minQualityJPEG	available range of values: 1–100	25	Specifies the image quality of the desktop display for JPEG/PNG encoding. The low-quality settings are for areas of the screen that change often, for example, when scrolling occurs.
RemoteDisplay.qpmaxH264	available range of values: 0–51	36	Use this option to set the H264minQP quantization parameter, which specifies the best image quality for the remote display configured to use H.264 or HEVC encoding. Set the value to greater than the value set for RemoteDisplay.qpminH264.
RemoteDisplay.qpminH264	available range of values: 0–51	10	Use this option to set the H264maxQP quantization parameter, which specifies the lowest image quality for the remote display configured to use H.264 or HEVC encoding. Set the value to less than the value set for RemoteDisplay.qpmaxH264.
RemoteDisplay.updateCacheSizeKB	An integer	256000	Use this option to set the maximum size, in kilobytes, of the encoder image cache. ■ The final size of the cache is the lesser of the value set here and the associated configuration of the client. ■ The final size of the cache cannot exceed half of the available RAM on the machine running Horizon Agent for Linux.
UsbRedirPlugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the USB Redirection plug-in.
UsbRedirServer.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the USB Redirection server.
vdpservice.log.logLevel	`fatal error`, `warn`, `info`, `debug`, or `trace`	`info`	Use this option to set the log level of the `vdpservice`.
viewusb.AllowAudioIn	**`{m|o}:{true|false}`**	undefined, which equates to `true`	Use this option to allow or disallow audio input devices to be redirected. Example: **`o:false`**
viewusb.AllowAudioOut	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to allow or disallow redirection of audio output devices.
viewusb.AllowAutoDeviceSplitting	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to allow or disallow the automatic splitting of composite USB devices. Example: **`m:true`**

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
viewusb.AllowDevDescFailsafe	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to allow or disallow devices to be redirected even if Horizon Client fails to get the configuration or device descriptors. To allow a device even if it fails to get the configuration or device descriptors, include it in the Include filters, such as **`IncludeVidPid`** or **`IncludePath`**.
viewusb.AllowHIDBootable	**`{m|o}:{true|false}`**	undefined, which equates to `true`	Use this option to allow or disallow the redirection of input devices other than keyboards or mice that are available at boot time, also known as HID-bootable devices.
viewusb.AllowKeyboardMouse	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Use this option to allow or disallow the redirection of keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad).
viewusb.AllowSmartcard	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to allow or disallow smart card devices to be redirected.
viewusb.AllowVideo	**`{m|o}:{true|false}`**	undefined, which equates to `true`	Use this option to allow or disallow video devices to be redirected.
viewusb.DisableRemoteConfig	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to deactivate or enable the use of Horizon Agent settings when performing USB device filtering.
viewusb.ExcludeAllDevices	**`{true|false}`**	undefined, which equates to `false`	Use this option to exclude or include all USB devices from being redirected. If set to **`true`**, you can use other policy settings to allow specific devices or families of devices to be redirected. If set to **`false`**, you can use other policy settings to prevent specific devices or families of devices from being redirected. If you set the value of **`ExcludeAllDevices`** to **`true`** on Horizon Agent, and this setting is passed to Horizon Client, the Horizon Agent setting overrides the Horizon Client setting.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
viewusb.ExcludeFamily	`{m|o}:family_name_1[;family_name_2;...]`	undefined	Use this option to exclude families of devices from being redirected. For example: `m:bluetooth;smart-card` If you have enabled automatic device splitting, Horizon 8 examines the device family of each interface of a composite USB device to decide which interfaces must be excluded. If you have deactivated automatic device splitting, Horizon 8 examines the device family of the whole composite USB device. **Note** Mice and keyboards are excluded from redirection by default. You do not have configure this setting to exclude mouse and keyboard devices.
viewusb.ExcludePath	`{m|o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2;...]`	undefined	Use this option to exclude devices at specified hub or port paths from being redirected. You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example:`m:bus-1/2/3_port-02;bus-1/1/1/4_port-ff`
viewusb.ExcludeVidPid	`{m|o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;..]`	undefined	Set this option to exclude devices with specified vendor and product IDs from being redirected. You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: `o:vid-0781_pid-****;vid-0561_pid-554c`
viewusb.IncludeFamily	`{m|o}:family_name_1[;family_name_2]...`	undefined	Set this option to include families of devices that can be redirected. For example: `o:storage; smart-card`
viewusb.IncludePath	`{m|o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../portz2;...]`	undefined	Use this option to include devices at specified hub or port paths that can be redirected. You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: `m:bus-1/2_port-02;bus-1/7/1/4_port-0f`

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
viewusb.IncludeVidPid	`{m|o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]`	undefined	Set this option to include devices with specified Vendor and Product IDs that can be redirected. You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: `o:vid-***_pid-0001;vid-0561_pid-554c`
viewusb.SplitExcludeVidPid	`{m|o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]`	undefined	Use this option to exclude or include a specified composite USB device from splitting by Vendor and Product IDs. The format of the setting is `vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]`. You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. Example: `m:vid-0f0f_pid-55**`
viewusb.SplitVidPid	`{m|o}:vid-xxxx_pid-yyyy([exintf:zz[;exintf:ww]])[;...]`	undefined	Set this option to treat the components of a composite USB device specified by Vendor and Product IDs as separate devices. The format of the setting is `vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])`. You can use the `exintf` keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (*) in place of individual digits in an ID. Example: `o:vid-0f0f_pid-***(exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)` **Note** Horizon 8 does not include the components that you have not explicitly excluded automatically. You must specify a filter policy such as **`Include VidPid Device`** to include those components.
VMWPkcs11Plugin.log.enable	`true` or `false`	`false`	Set this option to enable or deactivate the logging mode for the True SSO feature.
VMWPkcs11Plugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the True SSO feature.

Table 6-1. Configuration Options in `/etc/vmware/config` (continued)

	Value/Format	Default	Description
VVC.logLevel	`fatal error`, `warn`, `info`, `debug`, or `trace`	`info`	Use this option to set the log level of the VVC proxy node.
VVC.RTAV.Enable	`true` or `false`	`true`	Set this option to enable/deactivate Real-Time Audio-Video redirection.
VVC.RTAV.WebcamDefaultResHeight	available range of values: 32–2160	undefined	Use this option to set the default image height, in pixels, used for Real-Time Audio-Video redirection.
VVC.RTAV.WebcamDefaultResWidth	available range of values: 32–4096	undefined	Use this option to set the default image width, in pixels, used for Real-Time Audio-Video redirection.
VVC.RTAV.WebcamMaxFrameRate	available range of values: 1–30	undefined, which equates to no limit on the maximum frame rate	Use this option to set the maximum frame rate, in frames per second (fps), allowed for Real-Time Audio-Video redirection.
VVC.RTAV.WebcamMaxResHeight	available range of values: 32–2160	undefined, which equates to no limit on the maximum image height	Use this option to set the maximum image height, in pixels, allowed for Real-Time Audio-Video redirection.
VVC.RTAV.WebcamMaxResWidth	available range of values: 32–4096	undefined, which equates to no limit on the maximum image width	Use this option to set the maximum image width, in pixels, allowed for Real-Time Audio-Video redirection.
VVC.ScRedir.Enable	`true` or `false`	`true`	Set this option to enable/deactivate smart card redirection.

Configuration Options in /etc/vmware/viewagent-custom.conf

Java Standalone Agent uses the configuration file `/etc/vmware/viewagent-custom.conf`.

Table 6-2. Configuration Options in `/etc/vmware/viewagent-custom.conf`

Option	Value	Default	Description
CDREnable	`true` or `false`	`true`	Use this option to enable or deactivate the client drive redirection feature.
AppEnable	`true` or `false`	`true`	Use this option to enable or deactivate support for single-session application pools.
BlockScreenCaptureEnable	`true` or `false`	`false`	Use this option to prevent users from taking screenshots of their virtual desktop or published application from their end point using Windows or macOS devices.
CollaborationEnable	`true` or `false`	`true`	Use this option to enable or deactivate the Session Collaboration feature on Linux desktops.

Table 6-2. Configuration Options in `/etc/vmware/viewagent-custom.conf` (continued)

Option	Value	Default	Description
DPISyncEnable	`true` or `false`	`true`	Set this option to enable or deactivate the DPI Synchronization feature, which ensures that the DPI setting in the remote desktop matches the client system's DPI setting.
EndpointVPNEnable	`true` or `false`	`false`	Set this option to specify if the client's physical network card IP address or the VPN IP address is to be used when evaluating the endpoint IP address against the range of endpoint IP addresses used in the Dynamic Environment Manager Console. If you set the option to `false`, the client's physical network card IP address is used. Otherwise, the VPN IP address is used.
HelpDeskEnable	`true` or `false`	`true`	Set this option to enable or deactivate the Help Desk Tool feature.
KeyboardLayoutSync	`true` or `false`	`true`	Use this option to specify whether to synchronize a client's system locale list and current keyboard layout with Horizon Agent for Linux desktops. When this setting is enabled or not configured, synchronization is allowed. When this setting is deactivated, synchronization is not allowed. This feature is supported only for Horizon Client for Windows, and only for the English, French, German, Japanese, Korean, Spanish, Simplified Chinese, and Traditional Chinese locales.
LogCnt	An integer	-1	Use this option to set the reserved log file count in `/tmp/vmware-root`. ■ -1 - keep all ■ 0 - delete all ■ > 0 - reserved log count.
MaxSessionsBuffer	An integer between 1 and the value specified for **Max Sessions Per RDS Host** in the farm configuration wizard.	`5` or `1`	When configuring farms, use this option to specify the number of pre-launched sessions per host machine. When properly configured, this option can help speed the launch of desktop and application sessions. The default value is 5 for non-vGPU farms, 1 for vGPU farms. A higher value means that more resources are pre-consumed in a vGPU or non-vGPU environment. Configuring a high value is not recommended in a load-balanced vGPU environment that uses a lower vGPU profile because the high ratio of pre-consumed vGPU resources affects the behavior of the load balancer. For example, with a profile of 2Q in a load-balanced environment, using a high MaxSessionBuffer value can prevent the load balancer from assigning desktops and applications from that farm.
NetbiosDomain	A text string, in all caps	undefined	When configuring True SSO, use this option to set the NetBIOS name of your organization's domain.

Table 6-2. Configuration Options in `/etc/vmware/viewagent-custom.conf` (continued)

Option	Value	Default	Description
OfflineJoinDomain	`pbis` or `samba`	`pbis`	Use this option to set the instant-clone offline domain join. The available methods to perform an offline domain join are the PowerBroker Identity Services Open (PBISO) authentication and the Samba offline domain join. If this property has a value other than `pbis` or `samba`, the offline domain join is ignored.
PrintRedirEnable	`true` or `false`	`true`	Enables or deactivates the VMware Integrated Printing feature, which includes client printer redirection. **Note** To enable VMware Integrated Printing, you must set **both** of these configuration options to `true`: ■ `printSvc.enable` in `/etc/vmware/config` ■ `PrintRedirEnable` in `/etc/vmware/viewagent-custom.conf` If you set either one of these options to `false`, even with the other option set to `true`, VMware Integrated Printing is deactivated.
RunOnceScript	Script for joining the virtual machine to Active Directory	undefined	Use this option to rejoin the cloned virtual machine to Active Directory. Set the `RunOnceScript` option after the host name has changed. The specified script is run only once after the first host name change. The script runs with the root permission when the agent service starts and the host name has been changed since the agent installation. For example, for the winbind solution, you must join the base virtual machine to Active Directory with Winbind, and set this option to a script path. The script must contain the domain rejoin command `/usr/bin/net ads join -U <ADUserName>%<ADUserPassword>`. After VM Clone, the operating system customization changes the host name. When the agent service starts, the script executes to join the cloned virtual machine to Active Directory.
RunOnceScriptTimeout		120	Use this option to set the timeout time in seconds for the RunOnceScript option. For example, set `RunOnceScriptTimeout=120`
SSLCertName	A text string	vmwblast:cert	When deploying a VMwareBlastServer certificate with the `DeployBlastCert.sh` script, use this option to specify the certificate name as it will appear in the Linux keyring. For more information, see Install a CA-signed Certificate for VMwareBlastServer on a Linux Machine.

Table 6-2. Configuration Options in `/etc/vmware/viewagent-custom.conf` (continued)

Option	Value	Default	Description
SSLKeyName	A text string	vmwblast:key	When deploying a VMwareBlastServer certificate with the `DeployBlastCert.sh` script, use this option to specify the private key name as it will appear in the Linux keyring. For more information, see Install a CA-signed Certificate for VMwareBlastServer on a Linux Machine.
SSLCiphers	A text string	kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:TLS13-AES-256-GCM-SHA384:TLS13-AES-128-GCM-SHA256	Use this option to specify the list of ciphers used with TLSv1.1 and TLSv1.2. This option only takes effect if you specify TLSv1.1 or TLSv1.2 for `SSLProtocols`. The cipher list consists of one or more cipher strings in order of preference, separated by colons. The cipher string is case-sensitive. You must use the format defined by the OpenSSL standard. To find information about the OpenSSL-defined format, type these keywords into an Internet search engine: **`openssl cipher string`**.
SSLProtocols	A text string	TLSv1.3:TLSv1.2 (in non-FIPS mode) TLSv1.2 (in FIPS mode)	Use this option to specify the security protocols. The supported protocols are TLSv1.1, TLSv1.2, and TLSv1.3.
TLSCipherSuites	A text string	TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256	Use this option to specify the list of ciphers used with TLSv1.3. This option only takes effect if you specify TLSv1.3 for `SSLProtocols`. The cipher list consists of one or more cipher strings in order of preference, separated by colons. The cipher string is case-sensitive. You must use the format defined by the OpenSSL standard. To find information about the OpenSSL-defined format, type these keywords into an Internet search engine: **`openssl cipher string`**.

SSODesktopType	`UseGnomeClassic`
	or
	`UseGnomeFlashback`
	or
	`UseGnomeUbuntu`
	or
	`UseMATE`
	or
	`UseKdePlasma`
		undefined	This option specifies the desktop environment to use, instead of the default desktop environment, when SSO is enabled.
			You must first ensure that the selected desktop environment is installed on your desktop before specifying to use it. If you set this option in an Ubuntu desktop, the option takes effect regardless if the SSO feature is enabled or not. If you set this option in a RHEL/CentOS 7.x desktop, the selected desktop environment is used only if SSO is enabled.
			Note This option is not supported on RHEL 9.x/8.x desktops. Horizon 8 supports only the Gnome desktop environment on RHEL 9.x/8.x desktops.

SSOEnable	`true` or `false`	`true`	Set this option to enable/deactivate single sign-on (SSO).

Table 6-2. Configuration Options in `/etc/vmware/viewagent-custom.conf` (continued)

Option	Value	Default	Description
SSOUserFormat	A text string	[username]	Use this option to specify the format of the login name for single sign-on. The default is the user name only. Set this option if the domain name is also required. Typically, the login name is the domain name plus a special character followed by the user name. If the special character is the backslash, you must escape it with another backslash. Examples of login name formats are as follows: - SSOUserFormat=[domain]\\[username] - SSOUserFormat=[domain]+[username] - SSOUserFormat=[username]@[domain]
Subnet	A value in CIDR IP address format	[subnet]	When IPv4 support is enabled, set this option to an IPv4 subnet which other machines can use to connect to Horizon Agent for Linux. If there is more than one local IP address with different subnets, the local IP address in the configured subnet is used to connect to Horizon Agent for Linux. You must specify the value in CIDR IP address format. For example, Subnet=123.456.7.8/24.
Subnet6	A value in prefix/length IP address format	[subnet6]	When IPv6 support is enabled, set this option to an IPv6 subnet which other machines can use to connect to Horizon Agent for Linux. If there is more than one local IP address with different subnets, the local IP address in the configured subnet is used to connect to Horizon Agent for Linux. You must specify the value in prefix/length IP address format. For example, Subnet6=2001:db8:abcd:0012::0/64.
DEMEnable	`true` or `false`	`true`	Set this option to enable or deactivate smart policies created in Dynamic Environment Manager. In order for Dynamic Environment Manager policies to take effect, you must set this option to `true` and you must configure the **DEMNetworkPath** option. When Dynamic Environment Manager policies are in effect and the condition in a smart policy is met, then the policy is enforced.
DEMNetworkPath	A text string	undefined	You must set this option to the same network path set in the Dynamic Environment Manager Console. The path must be in the format similar to `//10.111.22.333/view/LinuxAgent/DEMConfig`. The network path must correspond to a public, shared folder which does not require user name and password credentials for access.

Note The VMwareBlastServer process uses the SSLCiphers, SSLProtocols, and SSLCipherServerPreference security options. When starting the VMwareBlastServer process, the Java Standalone Agent passes these options as parameters. When Blast Secure Gateway (BSG) is enabled, these options affect the connection between BSG and the Linux desktop. When BSG is not enabled, these options affect the connection between the client and the Linux desktop.

Configuration Settings in /etc/vmware/viewagent-greeter.conf

The settings in the `/etc/vmware/viewagent-greeter.conf` file support the True SSO and smart card SSO features. The settings also apply to the VMware greeter when SSO is deactivated. The configuration file includes two sections: **[SSOFailed]** and **[PKCS11]**.

The **defaultUsername** setting under **[SSOFailed]** specifies how the VMware greeter fetches the default user name in the event of a True SSO or smart card SSO failure.

The settings under **[PKCS11]** are used to fetch the default user name from the smart card certificate if smart card SSO authentication fails.

Note The **[PKCS11]** settings only take effect if you set **defaultUsername** to `false`.

Table 6-3. Configuration Settings in `/etc/vmware/viewagent-greeter.conf`

Section	Setting	Value/Format	Default	Description
[SSOFailed]	defaultUsername	`true` or `false`	`true`	Use this setting to specify how to get the user name when the single sign-on process fails. The behavior of this setting differs between True SSO and smart card SSO. **When True SSO fails -** ■ With `true`, the greeter gets the default user name that was used to log in to Horizon Connection Server. ■ With `false`, the greeter does not attempt to get a default user name. The user must manually enter a user name in the greeter screen. **When smart card SSO fails -** ■ With `true`, the greeter gets the default user name that was used to log in to Horizon Connection Server. ■ With `false`, the greeter gets the default user name from the certificate on the smart card, provided that the PKCS #11 settings in `/etc/vmware/viewagent-greeter.conf` are configured correctly. The greeter then prompts the user to enter the smart card PIN. **Note** The PKCS #11 settings only take effect when you set **defaultUsername** to `false`.
[SSOFailed]	scAuthTimeout	An integer	120	Use this setting to specify a timeout period, in seconds, for smart card SSO authentication. The following guidelines apply: ■ If you set the value to 0, smart card SSO authentication is attempted indefinitely, with no timeout. ■ If you leave this setting unconfigured, smart card SSO uses the default timeout of 120 seconds.
[PKCS11]	module	A file path	undefined	Use this setting to specify the path to the smart card driver. This setting is required.

Table 6-3. Configuration Settings in `/etc/vmware/viewagent-greeter.conf` (continued)

Section	Setting	Value/Format	Default	Description
[PKCS11]	slotDescription	A text string	undefined	Use this setting to specify the label of the slot used by the smart card reader. Specify "`none`" to use the first slot with an available authentication token. This setting is optional. **Note** You can specify the slot using either the `slotDescription` or `slotNum` setting. The following guidelines apply: ■ If you specify both settings, the `slotDescription` setting takes priority. ■ If you leave both settings unspecified, the greeter uses the first slot with an available token.
[PKCS11]	slotNum	An integer	-1 (no slot number is defined)	Use this setting to specify the slot number used by the smart card reader. This setting is optional. For information on how this setting relates to the `slotDescription` setting, see the previous entry in this table. **Note** Use this setting only if your PKCS #11 implementation can ensure consistent slot numbering.
[PKCS11]	service	A file path	undefined	Use this setting to specify the path to the PAM module used for smart card authentication. This setting is required.

Table 6-3. Configuration Settings in `/etc/vmware/viewagent-greeter.conf` (continued)

Section	Setting	Value/Format	Default	Description
[PKCS11]	mapper	A file path	undefined	Use this setting to specify the path to the Common Name (CN) mapper file used for smart card authentication. This setting is required.
[PKCS11]	waitForToken	An integer	10000	Use this setting to specify the period of time, in milliseconds (ms), allotted for detecting an authentication token in the smart card slot. If the greeter fails to detect a token within this time period, the current attempt is canceled and the greeter starts a new detection attempt. Observe the following: ■ If you set the value to -1, the greeter attempts to detect the token indefinitely, with no timeout. ■ If not configured, this setting uses the default timeout of 10000 ms.

Using Smart Policies

You can use Smart Policies to create policies that control the behavior of the USB redirection, clipboard redirection, and client drive redirection features on specific Linux desktops. To control the behavior of the digital watermark feature on specific Linux desktops, you use environment variables instead of Smart Policies.

You can create policies for user environment settings that control a range of behaviors. Horizon 8 Smart Policies for user environment settings are applied during login and can be refreshed during reconnect of a session. To reapply Horizon 8 Smart Policies when a user reconnects to a session, you can configure a triggered task.

With Smart Policies, you can create policies that take effect only if certain conditions are met. For example, you can configure a policy that deactivates the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

Requirements for Smart Policies

To use Smart Policies, your system environment must meet certain requirements.

- You must install Horizon Agent and VMware Dynamic Environment Manager 9.4 or later on a remote Windows desktop.
- Users must use Horizon Client to connect to remote Linux desktops that you manage with Smart Policies.

- The `DEMEnable` option must be enabled and the `DEMNetworkPath` option must be set in the `/etc/vmware/viewagent-custom.conf` file. See Edit Configuration Files on a Linux Desktop.
- You must install the client packages for accessing network shared storage. On an Ubuntu system, for example, install the `nfs-common` package for NFS-enabled shared storage and the `cifs-utils` package for Samba-enabled storage.

Installing Dynamic Environment Manager

To use Horizon Smart Policies to control the behavior of USB redirection, clipboard redirection, and client drive redirection on a remote Linux desktop, you must install Dynamic Environment Manager 9.4 or later on a remote Windows desktop.

You can download the Dynamic Environment Manager installer from the VMware Downloads page. You can install the Dynamic Environment Manager Management Console component on any Windows desktop from which you want to manage the Dynamic Environment Manager environment. From the Dynamic Environment Manager Management Console on a Windows desktop, you can control the behavior of remote desktop features on a remote Linux desktop.

For Dynamic Environment Manager system requirements and complete installation instructions, see the *Installing and Configuring VMware Dynamic Environment Manager* document.

Configuring Dynamic Environment Manager

You must configure Dynamic Environment Manager before you can use it to create smart policies for remote desktop features.

To configure Dynamic Environment Manager, follow the configuration instructions in the *VMware Dynamic Environment Manager Administration Guide*.

Horizon Smart Policy Settings

You control the behavior of remote features in Dynamic Environment Manager by creating a Horizon smart policy.

You can create policies for user environment settings that control a range of behaviors. Horizon Smart Policies for user environment settings are applied during login and can be refreshed during reconnect of a session. To reapply Horizon Smart Policies when a user reconnects to a session, you can configure a triggered task. See the complete list of policies in the topic "Configure Horizon Smart Policies for User Environment Settings" in the *VMware Dynamic Environment Manager Administration Guide*.

You can create policies for computer environment settings that Dynamic Environment Manager applies while end users' computers boot. Horizon Smart Policies for computer environment settings are applied during computer boot and can be refreshed during the reconnection of a session. See the complete list of policies in the topic "Configure Horizon Smart Policies for Computer Environment Settings" in the *VMware Dynamic Environment Manager Administration Guide*.

In general, Horizon smart policy settings that you configure for remote features in Dynamic Environment Manager override any equivalent registry key and group policy settings.

Adding Conditions to Horizon Smart Policy Definitions and Environment Variable Definitions

When you define a Horizon Smart Policy or environment variable in Dynamic Environment Manager, you can add conditions that must be met for the policy or variable to take effect. For example, you can add a condition that deactivates the client drive redirection feature only if a user connects to the remote desktop from outside your corporate network. Note that you can also enable a policy without adding conditions and the policy can still take effect.

Important You must add the following conditions to a Horizon Smart Policy or environment variable definition in order for the supported settings to take effect in a remote Linux desktop. These are the only conditions that are currently supported. If other conditions are set, the result of the condition evaluation is false.

Table 6-4. Required Conditions for Remote Linux Desktops

Condition	Description
`Operating System Architecture`	Checks the architecture of the operating system. The value must be set to **Linux**.
`Endpoint IP address`	Checks whether the endpoint IP address is in or not in the specified range. Empty fields at the start of the range are interpreted as 0, and the ones at the end as 255.
`Endpoint Platform`	Specifies the operating system of the user's client system. The remote display protocol must be set to **Blast/PCoIP**.
`Horizon Client Property`	This condition supports the client location property, which specifies the location of the user's client system. You can specify one of the following values: ■ **Internal**: The policy takes effect only if the client user connects to the remote desktop from within the corporate network. ■ **External**: The policy takes effect only if the client user connects to the remote desktop from outside the corporate network. For information about defining the internal and external network by setting the gateway location for a Connection Server, see "Configure the Gateway Location for a Horizon Connection Server in Horizon 8" in *Horizon Remote Desktop Features and GPOs*, which is part of the VMware Horizon Documentation. For information about defining the internal and external network by setting the gateway location for an Access Point appliance, see *Deploying and Configuring VMware Unified Access Gateway*, which is part of the Unified Access Gateway Documentation.

You can, however, set multiple `Endpoint IP address` conditions and combine them with other conditions, as shown in the following example.

```
Operating system is Linux

AND Endpoint IP address is in range 11.22.33.44 - 11.22.33.54
OR Endpoint IP address is in range 11.22.33.66 - 11.22.33.77
```

```
AND Blast/PCoIP endpoint platform is Windows

AND Horizon client property 'Client location' is equal to 'External'
```

For detailed information about adding and editing conditions in the Dynamic Environment Manager Management Console, see *VMware Dynamic Environment Manager Administration Guide*.

Create a Horizon Smart Policy in Dynamic Environment Manager

You use the Dynamic Environment Manager Management Console to create a Horizon smart policy in Dynamic Environment Manager. When you define a Horizon smart policy, you can add conditions that must be met for the smart policy to take effect.

Note To control the behavior of the digital watermark feature, you use environment variables instead of Horizon Smart Policies. See Set Up Digital Watermarks on a Linux Desktop With Environment Variables.

You can create policies for user environment settings that control a range of behaviors. Horizon Smart Policies for user environment settings are applied during login and can be refreshed during reconnect of a session. To reapply Horizon Smart Policies when a user reconnects to a session, you can configure a triggered task.

For complete information about using the Dynamic Environment Manager Management Console, see the *VMware Dynamic Environment Manager Administration Guide* document.

Prerequisites

- Install and configure Dynamic Environment Manager. See Installing Dynamic Environment Manager and Configuring Dynamic Environment Manager.
- Become familiar with the conditions that you can add to Horizon Smart Policy definitions. See Adding Conditions to Horizon Smart Policy Definitions and Environment Variable Definitions.
- Enable the `DEMEnable` option and configure the `DEMNetworkPath` option in the `/etc/vmware/viewagent-custom.conf` file. See Edit Configuration Files on a Linux Desktop.

Procedure

1 In the Dynamic Environment Manager Management Console, select the **User Environment** to create a policy for user environment settings or the **Computer Environment** tab to create a policy for computer environment settings.

  Existing Horizon smart policy definitions, if any, appear in the Horizon Smart Policies pane.

2 Select **Horizon Smart Policies** and click **Create** to create a new smart policy.

3 Select the **Settings** tab and define the smart policy settings.

   a In the General Settings section, enter a name for the smart policy in the **Name** text box.

   For example, if the smart policy affects the client drive redirection feature, you might name the smart policy CDR.

   b In the Horizon Smart Policy Settings section, select the remote desktop features and settings to include in the smart policy.

   You can select multiple remote desktop features.

4 Add the conditions required to use the new smart policy with remote Linux desktops.

   a Select the **Conditions** tab, click **Add**, and select the condition that you want to configure.

   For detailed information about configuring supported conditions and condition values, see Adding Conditions to Horizon Smart Policy Definitions and Environment Variable Definitions.

   b To add more conditions after configuring the first condition, click **Add** again.

   The **AND** operator is added by default to combine the conditions.

5 To save the smart policy, click **Save**.

Results

Dynamic Environment Manager processes the Horizon smart policy each time a user connects or reconnects to the remote desktop.

Dynamic Environment Manager processes multiple smart policies in alphabetical order based on the smart policy name. Horizon smart policies appear in alphabetical order in the Horizon Smart Policies pane. If smart policies conflict, the last smart policy processed takes precedence. For example, if you have a smart policy named Sue that enables USB redirection for the user named Sue, and another smart policy named Pool that deactivates USB redirection for the desktop pool named Ubuntu1804, the USB redirection feature is enabled when Sue connects to a remote desktop in the Ubuntu1804 desktop pool.

Note In a high-latency network, after saving your new or updated smart policy, allow Dynamic Environment Manager at least a minute to complete processing the changes before notifying the end users to connect to the affected desktops.

Set Up Digital Watermarks on a Linux Desktop With Environment Variables

You can configure environment variables in Dynamic Environment Manager to control the behavior of the digital watermark feature on specific Linux desktops.

Prerequisites

- Install and configure Dynamic Environment Manager. See Installing Dynamic Environment Manager and Configuring Dynamic Environment Manager.

- Enable the `DEMEnable` option and configure the `DEMNetworkPath` option in the `/etc/vmware/viewagent-custom.conf` file. See Edit Configuration Files on a Linux Desktop.

Configure Environment Variables in Dynamic Environment Manager

Use the following steps to configure environment variables that define the settings for a digital watermark on a Linux desktop.

1 In the Dynamic Environment Manager Management Console, click the **User Environment** tab and then select **Environment Variables**.

  Existing environment variable definitions, if any, appear in the Environment Variables pane.

2 To create a new environment variable, click **Create**.

3 Click the **Settings** tab and define the environment variable settings.

  a In the General Settings section, enter a name for the settings definition in the **Name** text box.

  b In the Environment Variable Settings section, enter the variable name and value exactly as described in the "Dynamic Environment Manager Environment Variable Values for the Digital Watermark Feature" section that follows this procedure.

4 Add the conditions required to use the environment variable with remote Linux desktops.

  a Select the **Conditions** tab, click **Add**, and select the condition that you want to configure.

    For detailed information about configuring supported conditions and condition values, see Adding Conditions to Horizon Smart Policy Definitions and Environment Variable Definitions.

  b To add more conditions after configuring the first condition, click **Add** again.

    The **AND** operator is added by default to combine the conditions.

5 To save the environment variable, click **Save**.

Repeat this procedure for each additional environment variable that you want to configure for digital watermark.

Note After saving your new or updated environment variables in a high-latency network, wait at least a minute while Dynamic Environment Manager finishes processing the changes before you make the affected desktops available to your end users.

Dynamic Environment Manager Environment Variable Values for the Digital Watermark Feature

In Dynamic Environment Manager, configure the environment variables described in the following table. Each environment variable maps to a corresponding configuration option in the `/etc/vmware/config` file. The environment variable settings take priority over the settings in `/etc/vmware/config`.

Environment variable	Corresponding option in /etc/vmware/config	Value/format of variable	Default	Description
WATERMARK	rdeSvc.enableWatermark	`0`: Deactivate `1`: Enable	`0`	Enables or deactivates the digital watermark feature. For information about the feature, see Features of Linux Desktops in VMware Horizon 8.

WATERMARK_FONT_NAME	rdeSvc.watermark.font	`serif`
		`sans-serif`
		`cursive`
		`fantasy`
		`monospace`
			`serif`	Defines the font used for the digital watermark.

WATERMARK_FONT_SIZE	rdeSvc.watermark.fontSize	An integer within the range of values: `8-72`	`12`	Defines the font size (in points) of the digital watermark.
WATERMARK_IMAGE_LAYOUT	rdeSvc.watermark.fit	`0`: Tile `1`: Center `2`: Multiple	`0`	Defines the layout of the digital watermark on the screen, which is divided into nine squares: ■ 0 = Tile: Watermark appears in all nine squares. Application sessions always use this layout. ■ 1 = Center: Watermark appears in the center square. ■ 2 = Multiple: Watermark appears in the center and four corner squares. If the watermark size exceeds the square size, it is scaled to maintain the aspect ratio.

Environment variable	Corresponding option in /etc/vmware/config	Value/format of variable	Default	Description
WATERMARK_MARGIN	rdeSvc.watermark.margin	An integer within the range of values: `0-1024`	`50`	Defines the amount of space (in pixels) around the digital watermark for the Tile layout. As the watermark scales, the margin also scales proportionally.
WATERMARK_OPACITY	rdeSvc.watermark.opacity	An integer within the range of values: `0-255`	`50`	Defines the transparency level of the digital watermark text.

WATERMARK_TEXT	rdeSvc.watermark.template	String constructed using any of the available information variables:
		`$BROKER_USER_NAME`
		`$BROKER_DOMAIN_NAME`
		`$USER_NAME`
		`$USER_DOMAIN`
		`$MACHINE_NAME`
		`$REMOTE_CLIENT_IP`
		`$CLIENT_CONNECT_TIME`
			`$USER_DOMAIN\`
			`$USER_NAME\n`
			`$MACHINE_NAME`
			`On`
			`$CLIENT_CONNECT_TIME`
			`\n$REMOTE_CLIENT_IP`
				Defines the text that you want to display for the digital watermark. Construct the watermark using any combination and order of the information variables. The character limit is 1024 characters and 4096 characters after expansion. The text is truncated if it exceeds the maximum length.

WATERMARK_TEXT_ROTATION	rdeSvc.watermark.rotation	An integer within the range of values: `0-360`	`45`	Defines the display angle of the digital watermark text.

Processing Order for Environment Variables

Dynamic Environment Manager processes environment variables each time a user connects or reconnects to the remote desktop.

Dynamic Environment Manager processes multiple environment variables in alphabetical order based on the environment variable name. Environment variables appear in alphabetical order in the Environment Variables pane. If several environment variables conflict, the last environment variable processed takes precedence. For example, if you have an environment variable named B that enables the watermark for the user named Sue, and another environment variable named A that deactivates the watermark for the desktop pool named Ubuntu 2204, the watermark is enabled when Sue connects to a remote desktop in the Ubuntu 2204 desktop pool.

Configure Screen-Capture Blocking Using Environment Variables

You can configure environment variables in Dynamic Environment Manager to control the behavior of the screen-capture blocking feature on specific Linux desktops.

Prerequisites

- Install and configure Dynamic Environment Manager. See Installing Dynamic Environment Manager and Configuring Dynamic Environment Manager.
- Enable the `DEMEnable` option and configure the `DEMNetworkPath` option in the `/etc/vmware/viewagent-custom.conf` file. See Edit Configuration Files on a Linux Desktop.

Configure Environment Variables in Dynamic Environment Manager

Use the following steps to the configure environment variable that defines the settings for screen-capture blocking on a Linux desktop.

1. In the Dynamic Environment Manager Management Console, click the **User Environment** tab and then select **Environment Variables**.

   Existing environment variable definitions, if any, appear in the Environment Variables pane.

2. To create a new environment variable, click **Create**.
3. Click the **Settings** tab and define the environment variable settings.

   a. In the General Settings section, enter a name for the settings definition in the **Name** text box.

   b. In the Environment Variable Settings section, enter the variable name and value exactly as described below. Each environment variable maps to a corresponding configuration option in the `/etc/vmware/viewagent-custom.conf` file. The environment variable settings take priority over the settings in `/etc/vmware/viewagent-custom.conf`.

Environment variable	Corresponding option in /etc/vmware/viewagent-custom.conf	Value/format of variable	Default	Description
BLOCK_SCREEN_CAPTURE_ENABLE	BlockScreenCaptureEnable	FALSE: Deactivate TRUE: Enable	FALSE	Enable/Deactivate Block Screen Capture. Default is FALSE

4. Add the conditions required to use the environment variable with remote Linux desktops.

   a. Select the **Conditions** tab, click **Add**, and select the condition that you want to configure.

   For detailed information about configuring supported conditions and condition values, see Adding Conditions to Horizon Smart Policy Definitions and Environment Variable Definitions.

   b. To add more conditions after configuring the first condition, click **Add** again.

The **AND** operator is added by default to combine the conditions.

5 To save the environment variable, click **Save**.

Note After saving your new or updated environment variable in a high-latency network, wait at least a minute while Dynamic Environment Manager finishes processing the changes before you make the affected desktops available to your end users.

Using DPI Synchronization with Linux Remote Desktops

This topic provides an overview of the DPI Synchronization feature for Linux remote desktops. The DPI Synchronization feature ensures that the DPI value in a remote session changes to match the DPI value of the client system when users connect to a remote desktop or published application.

The following considerations apply to the DPI Synchronization feature for Linux remote desktops and published applications.

- The **DPISyncEnable** configuration option in the `/etc/vmware/viewagent-custom.conf` file determines whether the DPI Synchronization feature is enabled for a desktop. The feature is enabled by default. For more information, see Edit Configuration Files on a Linux Desktop.
- To use DPI Synchronization on a client system with multiple monitors, configure each monitor with the same DPI setting. DPI Synchronization with a Linux remote desktop does not work if the client monitors have different DPI settings.
- DPI Synchronization is supported when users reconnect to a Linux remote desktop running in a Gnome desktop environment. Linux remote desktops running in a KDE or Mate desktop environment do not support DPI Synchronization upon reconnection. To use DPI Synchronization on a desktop running KDE or Mate, users must log out and log in to a new session.
- Gnome desktops do not support synchronization to the exact DPI values of the client system. Instead, DPI Synchronization rounds the client DPI value down to the nearest multiple of 96 for displaying the remote session. For example, suppose that the client system uses 250 DPI. Since 250 is greater than 192 (2 x 96) but less than 288 (3 x 96), the remote session uses the lower value, 192 DPI.

Table 6-5. DPI Synchronization Values for Gnome Desktops

Client DPI	Remote Session DPI
96–191	96 (1 x 96)
192–287	192 (2 x 96)
288–383	288 (3 x 96)
384–479	384 (4 x 96)

Configure VMware Integrated Printing for Linux Desktops

With VMware Integrated Printing, users can print from a Linux remote desktop to any local or network printer available on their client device. VMware Integrated Printing works with desktop client devices running Horizon Client or HTML Access.

VMware Integrated Printing supports client printer redirection, which is described in detail later in this article. VMware Integrated Printing also supports the ability to include a watermark with printed jobs, as described in Add Watermarks With VMware Integrated Printing on Linux Desktops.

VMware Integrated Printing is only supported on Linux desktops running RHEL 7.9/8.x/9.x, Rocky Linux 8.x/9.x, Ubuntu 20.04.x/22.04.x, or Debian 10.x/11.x/12.x.

Install and Enable VMware Integrated Printing

By default, VMware Integrated Printing is installed and enabled when you install Horizon Agent on a Linux machine. The feature does not require any custom installation or configuration options for activation.

If needed, you can use the **printSvc.enable** configuration option in the `/etc/vmware/config` file or the **PrintRedirEnable** configuration option in the `/etc/vmware/viewagent-custom.conf` file to deactivate VMware Integrated Printing. See Edit Configuration Files on a Linux Desktop.

Client Printer Redirection

With client printer redirection, users can print from a remote desktop to any local or network printer available on their client computer. The client printer is redirected to the remote desktop to process the print job. You do not need to install any printer driver on the remote desktop.

VMware Integrated Printing supports the following types of printer drivers on the client side:

- For printers redirected from a Windows client to the remote desktop, VMware Integrated Printing supports Universal Printer Driver (UPD).
- For printers redirected from a Mac or Linux client to the remote desktop, VMware Integrated Printing supports Native Printer Driver (NPD).
- For printers redirected from a Chrome client or HTML Access to the remote desktop, VMware Integrated Printing supports Universal Printer Driver (UPD). To print from a remote desktop, follow this workflow:

  a Select **Horizon_Printer(v*xx*)** in the first print dialog box.

  b Then select a redirected printer from the second print dialog box that appears. The options specified in the second print dialog box override the options specified in the first print dialog box.

Static Printer Names

Redirected printers retain their names across sessions so that users do not need to remap the printer manually when they connect to another session. The redirected printer appears with one of the following suffixes appended to the printer name:

- For a single-session desktop or application, the suffix is `(vdi + session ID - connection ID)`.
- For a multi-session desktop or application, the suffix is `(v + session ID - connection ID)`.

Universal Printer Driver Print Settings

VMware Integrated Printing provides the following print settings for redirected UPD printers from Windows clients.

- **Orientation**: select portrait or landscape orientation of the paper. The staple and punch finishing options depend on the orientation of the paper.
- **Print on Both Sides**: select duplex (double-sided) printing for duplex-capable printers.
- **Multiple Pages per Sheet**: to print multiple document pages onto one physical page, select the number of pages to print onto one physical page, and select the layout of the pages.
- **Paper size**: select the paper size:
  - Standard paper sizes: paper sizes that most printers commonly support, such as A4, letter, and legal.
  - Vendor-defined paper sizes (also called nonstandard paper sizes): paper sizes that are defined by a printer vendor.
  - User-defined paper sizes (also called customized paper sizes): paper sizes that are defined by system administrators.
- **Color**: specify whether a color printer prints color or monochrome.
- **Number of copies**: specify the number of copies.

Exclude Printers From VMware Integrated Printing

To configure filters for client printers, you can use the **printSvc.printerFilter** option in the `/etc/vmware/config` file. Printers specified in the filter are excluded from redirection and do not appear as available printers on the Linux desktop.

printSvc.printerFilter supports search query syntax that lets you filter printers based on the name of the printer, the driver, or the driver vendor. See Edit Configuration Files on a Linux Desktop.

Configure Default Print Options

You can use the **printSvc.defaultPrintOptions** option in the /etc/vmware/config file to specify the default print settings used to print output, if print settings cannot be detected from the source application. See Edit Configuration Files on a Linux Desktop.

Note The **printSvc.defaultPrintOptions** configuration option is only supported for Windows, Linux, and Mac clients.

Customize the List of Available Paper Sizes

To customize the list of paper sizes that can be used for printing output through VMware Integrated Printing, you must create a properly formatted configuration file that defines the paper sizes. Then use the **printSvc.paperListFile** option in the /etc/vmware/config file to specify the file path to that configuration file of paper sizes. Only the paper sizes listed in the configuration file are available as options when printing.

See Edit Configuration Files on a Linux Desktop.

Note VMware Integrated Printing supports customized paper-size lists only when printing from Windows clients. The feature applies globally to all redirected printers on a Windows client system.

Redirect Non-NPD and Non-UPD Printers

To redirect a client printer that does not use an NPD or UPD driver, you must install the printer's custom PPD file on the agent machine. Then use the **printSvc.customizedPpd** configuration option in the /etc/vmware/config file to specify the file path to that PPD file. See Edit Configuration Files on a Linux Desktop.

Configure PDF as the Print Format

You can use the **printSvc.usePdfFilter** configuration option in the /etc/vmware/config file to specify whether or not to use PDF as the print format for redirected printers. See Edit Configuration Files on a Linux Desktop.

Note The **printSvc.usePdfFilter** configuration option is only supported for Linux and Mac clients.

Configure a Printed Watermark

VMware Integrated Printing supports the ability to include a watermark with printed jobs. For information about this feature, see Add Watermarks With VMware Integrated Printing on Linux Desktops.

Event Log for VMware Integrated Printing

You can find the event log for VMware Integrated Printing at /tmp/vmware-$user/vmware-PrintRedir-*xxx*.log.

To specify the level of detailed reported in the event log, use the **printSvc.logLevel** configuration option in the `/etc/vmware/config` file. See Edit Configuration Files on a Linux Desktop.

Add Watermarks With VMware Integrated Printing on Linux Desktops

With VMware Integrated Printing, you can add a watermark to jobs printed from a remote Linux session. You can customize the text content and format of the watermark using advanced print options.

Prerequisites

To enable the VMware Integrated Printing watermark feature, you must perform the following prerequisite tasks.

- In the `/etc/vmware/config` file, set the **printSvc.watermarkEnabled** configuration option to **`true`**. See Edit Configuration Files on a Linux Desktop.
- Install the QPDF package on the agent machine, as described in the following procedures.

Install QPDF on a RHEL 9.x or Rocky Linux 9.x Machine

1 Enable the Extra Packages for Enterprise Linux (EPEL).

```
yum -y install https://dl.fedoraproject.org/pub/epel/epelrelease-latest-9.noarch.rpm
```

2 Enable the CodeReady Linux Builder (CRB) repository.

```
/usr/bin/crb enable
```

3 Install the QPDF package.

```
dnf install qpdf
```

Install QPDF on a RHEL 8.x Machine

1 Install and enable gcc-toolset.

```
yum install -y gcc-toolset-12
scl enable gcc-toolset-12 bash
```

2 Install the zlib-devel and libjpeg-turbo-devel packages.

```
yum install -y zlib-devel libjpeg-turbo-devel
```

3 Download and build the QPDF package.

```
wget https://github.com/qpdf/qpdf/releases/download/release-qpdf-10.3.1/qpdf-10.3.1.tar.gz
tar -zxvf qpdf-10.3.1.tar.gz
```

```
cd qpdf-10.3.1
./configure
make
make install
```

Install QPDF on a CentOS 7.9 Machine

1 Enable the Red Hat Software Collections (RHSCL).

```
yum-config-manager --enable rhel-workstation-rhscl-7-rpms
```

2 Install and enable the Red Hat Developer Toolset.

```
yum install devtoolset-7
scl enable devtoolset-7 bash
```

3 Install the zlib-devel and libjpeg-turbo-devel packages.

```
yum install -y zlib-devel libjpeg-turbo-devel
```

4 Download and build the QPDF package.

```
wget https://github.com/qpdf/qpdf/releases/download/release-qpdf-10.3.1/qpdf-10.3.1.tar.gz
tar -zxvf qpdf-10.3.1.tar.gz
cd qpdf-10.3.1
./configure
make
make install
```

Install QPDF on an Ubuntu/Debian Machine

- Run the command to install the QPDF package.

```
apt install qpdf
```

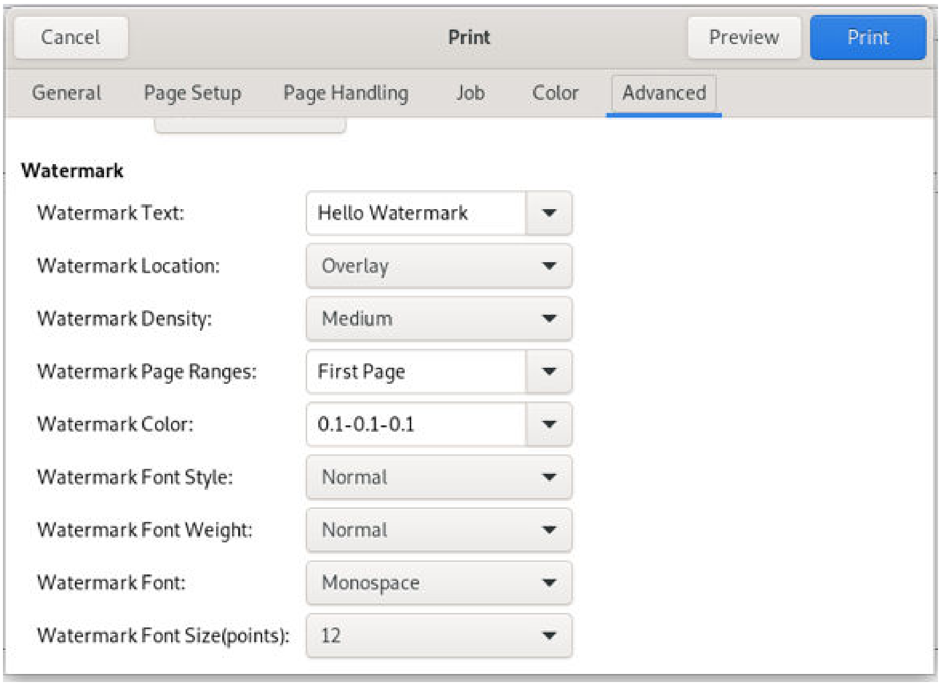
Configure the Printed Watermark Settings

You can use print options to specify the content and format of the watermark.

Note The watermark is always printed in a repeating pattern on lines parallel to the diagonal of the page.

1 Open the print dialog box for the job you want to print.

2 Select the **Advanced** tab.



Watermark

Watermark Text: Hello Watermark

Watermark Location: Overlay

Watermark Density: Medium

Watermark Page Ranges: First Page

Watermark Color: 0.1-0.1-0.1

Watermark Font Style: Normal

Watermark Font Weight: Normal

Watermark Font: Monospace

Watermark Font Size(points): 12

3 Configure the watermark options as described in the following table.

Option	Allowed Values	Description
Watermark Text	Unicode text characters	Text content of the printed watermark.
Watermark Location	**Overlay**, **Underlay**	Placement of the watermark in relation to the page content. ■ **Overlay** places the watermark in front of the printed page content. ■ **Underlay** places the watermark behind the printed page content.
Watermark Density	**Low**, **Medium**, **High**	The density level, or number of rows used to print the watermark. ■ **Low** repeats the watermark in a single row along the diagonal of the page. ■ **Medium** repeats the watermark in several rows parallel to the diagonal of the page. ■ **High** repeats the watermark in many rows parallel to the diagonal of the page.
Watermark Page Ranges	**All Pages**, **First Page**, or a custom page range	The pages on which to include the watermark. To specify a custom page range, use commas to separate non-consecutive pages and hyphens to indicate a consecutive range. For example: "1,3,4-5,99-200"
Watermark Color	**Blue**, **Gray**, **Red**, or a custom color specified as arithmetic RGB values	The color of the watermark. To specify a custom color, use the format *<R value>-<G value>-<B value>*, where the values represent the intensities of the red, green, and blue components of the color. Each value can range from 0.0 (lowest intensity) to 1.0 (highest intensity). For example: "0.31-0.42-0.55"

Option	Allowed Values	Description
Watermark Font Style	**Normal**, **Italic**, **Oblique**	The typeface style, or slope, of the watermark.
Watermark Font Weight	**Thin**,**Ultralight**, **Light**, **Semilight**, **Book**, **Medium**, **Semibold**, **Bold**, **Ultrabold**, **Heavy**, **Ultraheavy**	The stroke weight, or thickness, of the watermark font. The effect of each weight value depends on the font selected.
Watermark Font	Any system-supported font	The typeface used to print the watermark.
Watermark Font Size	An integer from 6 through 96	The size, in points, of the watermark font. If the specified size exceeds the printed page dimensions, VMware Integrated Printing automatically adjusts to the nearest point value that can fit the watermark on the page.

Example Blast Settings for Linux Desktops

You can adjust the image quality of your remote desktop display to improve the user experience. Improving image quality is helpful in maintaining a consistent user experience when network connection is less than optimal.

Video Encoders Used for Desktop Sessions

The video encoder used for a desktop session depends on the capabilities of both the desktop and client systems. When a user opens a session, Horizon 8 evaluates the hardware and software capabilities of the desktop and client and selects the highest-priority encoder that is supported by both.

For example, Horizon 8 uses HEVC if all the following components are configured to support or allow HEVC:

- The Linux desktop system
- Horizon Agent on the Linux desktop
- The client system
- Horizon Client on the client system

If any one of the components does not support HEVC, Horizon 8 selects the next encoder on the priority list that is supported by all the components.

For a session that uses vGPU technology, Horizon 8 selects from the following encoders listed in order of priority:

1. HEVC YUV 4:4:4
2. H.264 YUV 4:4:4
3. HEVC

4 H.264

5 Switch Encoder

6 BlastCodec

For a non-vGPU session, Horizon 8 selects from the following priority list of encoders:

1 Switch Encoder

2 H.264

3 BlastCodec

Example VMware Blast Extreme Protocol Settings

VMwareBlastServer and its related plug-ins use the configuration file `/etc/vmware/config`.

Table 6-6. Example Blast Configuration Options in `/etc/vmware/config`

Option name	Parameter	High-speed LAN	LAN	Dedicated WAN	Broadband WAN	Low-speed WAN	Extremely Low speed
Bandwidth settings	RemoteDisplay.maxBandwidthKbps	1000000 (1 Gbps)	1000000 (1 Gbps)	1000000 (1 Gbps)	5000 (5 Mbps)	2000 (2 Mbps)	1000 (1 Mbps)
Max FPS	RemoteDisplay.maxFPS	60	30	30	20	15	5
Audio Playback	RemoteDisplay.allowAudio	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE
Display Quality (JPEG/PNG)	RemoteDisplay.maxQualityJPEG	90	90	90	70	60	50
Display Quality (JPEG/PNG)	RemoteDisplay.midQualityJPEG	35	35	35	35	35	35
Display Quality (JPEG/PNG)	RemoteDisplay.minQualityJPEG	25	25	25	20	20	20
Display Quality (H.264 or HEVC)	RemoteDisplay.qpmaxH264	28	36	36	36	36	42
Display Quality (H.264 or HEVC)	RemoteDisplay.qpminH264	10	10	10	10	10	10

Examples of Client Drive Redirection Options for Linux Desktops

Configure client drive redirection (CDR) options to determine whether a local system's shared folders and drives can be accessed from the remote Linux desktops.

Configure CDR settings by adding entries to the `/etc/vmware/config` file.

The following configuration example shares the `d:\ebooks` and `C:\spreadsheets` folders, makes both folders read-only, and prevents the client from sharing more folders.

```
cdrserver.forcedByAdmin=true
cdrserver.sharedFolders=d:\ebooks,;c:\spreadsheets,
cdrserver.permissions=R
```

In the previous example, the comma **","** placed after **ebooks** and **spreadsheets** is mandatory for correct option parsing.

Any **"R"** included in the `cdrserver.sharedFolders`option would impact all the folders listed in that setting. In the following example, the **ebooks** and **spreadsheets** folders are both read-only even if the **R** value is only placed after **/home/jsmith** folder path.

```
cdrserver.sharedFolders=d:\ebooks,;c:\spreadsheets,;/home/jsmith,R
```

Creating and Managing Instant-Clone Desktop Pools 7

To provide users access to instant-clone desktops, you must create an instant-clone desktop pool.

Read the following topics next:

Instant Clone Desktop Pools

An instant clone desktop pool is an automated desktop pool created from a golden image using the vmFork technology (called the instant clone API) in vCenter Server.

Instant clone replaces View Composer linked clone as the process for creating non-persistent and persistent desktops in Horizon 8. In addition to using the instant clone API from vCenter Server, Horizon 8 also creates several types of internal VMs (Internal Template, Replica VM, and Parent VM) to manage these clones in a more scalable way.

Instant clones share the virtual disk of the parent VM and consume less storage than full VMs. In addition, instant clones share the memory of the parent VM when they are first created, which contributes to fast provisioning. As users log into these cloned desktops, additional memory is consumed.

While the use of a parent VM is helpful in improving the provisioning speed, it does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon 8 automatically chooses to provision instant clones directly from a replica VM without creating any parent VM. This feature is called Smart Provisioning. Smart Provisioning creates instant clones using one of the following provisioning schemes:

- Mode A - Instant clones with parent VM
- Mode B (Default) - Instant clones without parent VM

Smart Provisioning will select Mode A only when using a vTPM device on ESXi hosts with versions older than 7.0 update 3f. You can still set the provisioning mode by setting `pae-ProvisionScheme` attribute in ADAM database. See https://kb.vmware.com/s/article/81026 for details.

A single instant clone desktop pool can have instant clones that are created with or without parent VMs.

Computer-based group policy objects (GPOs) that require a reboot on a golden image Windows VM do not apply to instant clones because instant clones are created in a powered-on state. To apply the golden image VM GPOs to instant clones, see Applying Computer-based GPOs that Require Reboot on Windows Instant Clones below.

Instant clone desktop pools have the following benefits:

- The provisioning of instant clones is fast.
- Instant clones are always created in a powered-on state, ready for users to connect. Guest customization and joining the Active Directory domain are completed as part of the initial power-on workflow.
- You can patch a pool of instant clones in a rolling process with zero downtime.

Compute Profiles for Instant Clone Desktop Pools

A compute profile of an instant clone desktop pool is the number of vCPUs and vRAM allocated to each desktop in a pool. When creating an instant clone desktop pool, the administrator must specify the golden image and snapshot, as described in the Worksheet for Creating an Instant-Clone Desktop Pool. By default, Horizon 8 inherits the compute profile of the selected snapshot to create the desktop pool.

Previously, if an administrator wanted to create two different pools of instant clone virtual desktops that use the same OS image but have different VM compute profiles, they had to create and maintain two golden images or two snapshots. This complicated the management of images and made patch updates more time-consuming.

With the compute profile feature, administrators can override the default compute profile and specify the desired vCPU, vRAM, and cores per socket to create the desktop pool. In this way, the same golden image and snapshot can be used to create multiple desktop pools where each pool has a different VM compute profile.

Administrators can change the compute profile for a pool during one of the following workflows:

- Create an Instant-Clone Desktop Pool
- Patching an Instant-Clone Desktop Pool
- Selective Patching of Virtual Machines

Applying Computer-based GPOs that Require Reboot on Windows Instant Clones

Some computer-based GPOs are processed at Windows startup and typically require a reboot for them to be applied to the desktop. To apply these GPOs properly to instant clones, follow these steps:

1 Create or update the computer-based policy settings in the target OU for the instant-clone desktops.

2 Take a new snapshot of the existing parent VM (or create a new parent VM) in vCenter Server. Even if nothing has changed on the parent VM, this will publish a new base image for the clones, which then receive the GPOs created in the previous step.

3 In the administration console, push a new image to update the existing pool (or create a new pool) of instant clones using the parent VM in vCenter Server and the new snapshot created in the previous step. The GPOs are then applied to the instant clones.

Note the following:

- Changes to foreground GPOs always require re-publishing as described in the preceding steps.
- To ensure that background policies are applied before user login, apply `Always wait for the network at computer startup and logon ** and re-publish` as described in the group solution policy. This policy is located at `Computer Configuration\Administrative Templates\System\Logon`.

Instant-Clone Image Publishing and Creation Workflow

Publishing an image is a process by which internal VMs needed for instant cloning are created from a golden image and its snapshot. This process only happens once per image and may take some time.

VMware Horizon 8 performs the following steps to create a pool of instant clones:

1 Horizon 8 publishes the image that you select. In vCenter Server, four folders (`ClonePrepInternalTemplateFolder`, `ClonePrepParentVmFolder`, `ClonePrepReplicaVmFolder`, and `ClonePrepResyncVmFolder`) are created if they do not exist, and some internal VMs that are required for cloning are created. In Horizon Console, you can see the progress of this operation on the **Summary** tab of the desktop pool. During publishing, the Pending Image pane shows the name and state of the image.

   Note Do not tamper with the four folders or the internal VMs that they contain. Otherwise, errors might occur. The internal VMs are removed when they are no longer needed. Normally the VMs are removed within 5 minutes of pool deletion or a push-image operation. However, sometimes the removal can take up to 30 minutes. If there are no internal VMs in all four folders, these folders are unprotected and you can delete these folders.

2 After the image is published, Horizon 8 creates the instant clones. This process is fast. During this process, the Current Image pane in Horizon Console shows the name and state of the image.

   Note The unprime task of the Instant Clone creation workflow is now configurable and can be changed if you are having time-out issues when using vGPU-enabled VMs at this location. Use the new LDAP setting `cs-UnprimeImageTimeoutMins` to change the default timeout value of 30 minutes. See VMware KB 96141 for details.

After the pool is created, you can change the image through the push-image operation. As with the creation of a pool, the new image is first published. Then the clones are recreated.

When an instant clone pool is created, Horizon 8 spreads the pool across datastores automatically in a balanced way. If you edit a pool to add or remove datastores, rebalancing of the cloned desktops happens automatically when a new clone is created.

Worksheet for Creating an Instant-Clone Desktop Pool

When you create an instant-clone desktop pool, you can configure certain options. Use this worksheet to record your configuration options before you create the pool.

Before creating an instant-clone desktop pool, take a snapshot of the golden image. You must shut down the golden image in vCenter Server before taking the snapshot.

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool

Option	Option	Description	Enter Your Value Here
Type	Select **Automated Desktop Pool**.		
vCenter Server	Select **Instant Clone** and select the vCenter Server that manages the instant-clone VMs.		
User assignment		The following settings determine how end users are assigned to the desktops in this pool.	
	Select **Floating** or **Dedicated**.	In a floating instant-clone desktop pool, users are assigned random desktops from the pool. When a user logs out, the instant-clone desktop VM is deleted. A new clone is then regenerated using the latest golden image, based on the pool provisioning setting. In a dedicated instant-clone desktop pool, users are assigned a specific remote desktop and return to the same desktop at each login. When a user logs out, a refresh operation retains the computer name and the MAC address of the VM, deletes the desktop clone, and regenerates a new desktop clone from the latest golden image with the retained computer name and MAC address. You can optionally configure the instant-clone desktop pool to not refresh after logout.	
	Enable Automatic Assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user. For more information, see Assign a Machine to a User in a Dedicated-Assignment Pool.	
	Enable Multi-User Assignment	In a dedicated-assignment pool, you can assign multiple users to each machine in the pool. Multi-user assignment is not supported for automatic user assignment. Persistent disks do not support a multi-user assignment. If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users will be unable to launch a session on that machine. For more information, see Assign a Machine to a User in a Dedicated-Assignment Pool.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
Storage Optimization	Storage Policy Management: ■ **Use VMware Virtual SAN** ■ **Do not use VMware Virtual SAN**	Specify whether to use VMware vSAN, if available. vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts.	
	Select separate datastores for replica and OS disks	Specify whether to store the replica and OS disks on a datastore that is different from the datastores that the instant clones are on. If you select this option, you can select the options to select one or more instant-clone datastores or replica disk datastores.	
	Persistent Disk	This feature is available for Windows dedicated desktops only. Persistent disks allow you to preserve user data and settings when the instant clone is updated, refreshed, or rebalanced. **Redirect Windows Profile to a Persistent Disk** Select this option to store data on a separate persistent disk. ■ **Disk size** Provide the disk size in megabytes. ■ **Drive letter** Provide the drive letter. **Do not redirect Windows profile** Select this option to store the Windows profile in the OS disk. This feature does not support a multi-user assignment.	
Desktop Pool Identification		The following settings allow you to identify and describe the pool you are creating.	
	ID	The unique name that identifies the desktop pool. If you have multiple Connection Server configurations, make sure that another Connection Server configuration does not use the same pool ID. A Connection Server configuration can consist of a single Connection Server or multiple Connection Servers	
	Display name	The pool name that users see when they log in from a client. If you do not specify a name, the pool ID is used.	
	Access group	Select an access group for the pool or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. **Note** Access groups are different from vCenter Server folders that store desktop VMs. You select a vCenter Server folder later in the wizard.	
Provisioning Settings		The following settings allow you to provide details on how the pool is provisioned.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Enable Provisioning	You can enable or deactivate virtual machine provisioning in the desktop pool. When you deactivate provisioning in the desktop pool, Horizon 8 stops provisioning new virtual machines for the desktop pool. After you deactivate provisioning, you can enable provisioning again. Before you change a desktop pool's configuration, you can deactivate provisioning to ensure that no new machines are created with the old configuration. You can also deactivate provisioning to prevent Horizon 8 from using additional storage when a pool is close to filling up the available space. When you first create a desktop pool and deactivate this option, Horizon 8 creates a desktop pool without any virtual machines. If you edit a desktop pool and deactivate provisioning, Horizon 8 does not allow any new virtual machines to be provisioned in this desktop pool. End users can still connect to existing virtual machines. For instant-clone desktop pools that are configured to refresh after a user logs out, Horizon 8 deletes the old clone and creates a new clone to replace. This operation will continue to work even if you have deactivated pool provisioning.	
	Stop provisioning on Error	Specify whether Horizon 8 stops provisioning desktop VMs if an error occurs and prevents the error from affecting multiple VMs.	
	Virtual Machine Naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines.	
	Specify names manually	Enter names that will be used to create new virtual machines. Each line must contain a unique machine name. Optionally, for dedicated desktop pools, a user name can be specified. Specific user names will be ignored for floating desktop pools.	
	# Unassigned Machines Kept Powered On	The number must be a valid integer greater than 0 and less than or equal to the maximum number of names specified. The default is 1. This option is available for dedicated pools with virtual machines specified manually and is not available for floating pools	
	Naming Pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine. See Using a Naming Pattern for Desktop Pools.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Provision Machines - Machines on Demand: Min number of machines - All Machines Up-Front	Specify whether to provision all desktop VMs when the pool is created or to provision the VMs when they are needed. - **Machines on demand**. When the pool is created, Horizon 8 creates the number of VMs based on the **Min number of machines** value or the **Number of spare (powered on) machines** value, whichever is higher. Additional VMs are created to maintain this minimum number of available VMs as more users connect to desktops. This provides dynamic pool expansion capability where the size of the pool expands and contracts to accommodate the number of users who need desktops. When Horizon 8 is deployed on VMware Cloud on AWS, you can configure the Elastic DRS feature (rapid scaling) so that additional hosts can be automatically created (and conversely decommissioned) to meet the capacity required by the desktop pool. For more information about VMware Cloud on AWS, see the VMware Cloud on AWS documentation at https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html. **Note** Provisioning machines on demand is only available for machines that use a naming pattern. It is turned off for virtual machines whose names are specified manually in both dedicated and floating pools. - **All machines up front**. When the pool is created, Horizon 8 provisions the number of VMs you specify in **Max number of machines**. For a floating desktop pool, the MAC address is preserved on a resync or refresh.	
	Desktop Pool Sizing: Maximum Machines	Specify the maximum number of desktop VMs and powered-on spare machines in the pool. For details, see Naming Machines Manually or Providing a Naming Pattern in Horizon Console.	
	Desktop Pool Sizing: Spare (Powered On) Machines	Specify the number of desktop VMs to keep available to users. For details, see Naming Machines Manually or Providing a Naming Pattern in Horizon Console.	
	Virtual Device: Add vTPM Device to VMs	Select the checkbox to add a Virtual Trusted Platform Module (vTPM) device to VMs. This option does not apply to Linux VMs.	
vCenter Settings		The following settings describe vCenter attributes for the pool of desktops.	
	Golden Image in vCenter	Select the golden image in vCenter Server for the pool.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Snapshot	Select the snapshot you took of the golden image. To specify the number of monitors and resolution for your instant-clone desktop pool, you must configure these parameters in the golden image and then take a snapshot. See Configure Monitors and Screen Resolution for Instant Clones.	
	VM Folder Location	Select the folder in vCenter Server for the desktop VMs.	
	Cluster	Select the vCenter Server cluster for the desktop VMs.	
	Resource pool	Select the vCenter Server resource pool for the desktop VMs.	
	Datastores	Select one or more datastores for the desktop VMs. The **Select Instant Clone Datastores** window provides high-level guidelines for estimating the pool's storage requirements. These guidelines help you determine which datastores are large enough to store the clones. The Storage Overcommit value is always set to Unbounded and is not configurable. **Note** Instant clones and Storage vMotion are compatible. When you create an instant-clone desktop pool on a Storage DRS datastore, the Storage DRS cluster does not appear in the list of datastores. However, you can select individual Storage DRS datastores.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Networks	Select the networks to use for the instant-clone desktop pool. You can select multiple vLAN networks to create a larger instant-clone desktop pool. This option uses the network type from the golden image that was selected to create the pool and displays networks based on the network type of the golden image. You can use the same network as the selected golden image or select a network from the list of available options. Networks are filtered based on the golden image network type and the networks available in the selected cluster. The **Select Networks** wizard provides a list of networks based on the golden image's preferred network adapter (Network Adapter 1) network type: Standard, NSX Opaque Network, NSX-V, CVDS, 4.x+ and DVS. To use multiple networks for a network adapter, you must deselect **Use network from golden image** (which uses the network and network type from the selected golden image) and then select the networks to use with the new pool. The **Show all networks for each network adapter** switch shows or hides (dims) incompatible networks for all network types. By default, only compatible networks are shown. **Important** If you already have another pool using same parent and same golden image but created with different networks than the golden image, the new instant-clone pool will not use the golden image network as expected. To avoid this outcome, select the **Show All Networks** option and then manually select the desired network. **Note** You can select any one available Standard network per network adapter. Using more than one Standard network per network adapter is not supported. The wizard displays error messages for the following incompatible networks: ■ **vmcNetworks** - The network belongs to the VMC internal network. ■ **dvsUplinkPort** - The network does not meet the naming standards for a virtual switch uplink port. ■ **notConfiguredOnAllHosts** - The network is not configured on all hosts in the cluster. The wizard also provides the list of ports and port bindings that are available to use: static (early binding) and ephemeral. All selected NSX-t network segments must be the same size, such as all /24 networks. Unequal sized segments can result in provisioning errors. See the video below this table and https://kb.vmware.com/s/article/90569 for additional information.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	CPU	Update the default CPU if desired. - The default value is taken from the selected snapshot in vCenter Server. - You can update this value again in the future using the Push Image function. **Note** The CPU value must be a multiple of the Cores per Socket value.	
	RAM	Update the default RAM if desired. - The default value is taken from the selected snapshot in vCenter Server. - You can update this value again in the future using the Push Image function. **Note** If you set a memory reservation on the golden image VM through vSphere Client, use the "Reserve all guest memory (All locked)" option to ensure the correct behavior when creating pools with different values of RAM than the golden image.	
	Cores per Socket	Update the default Cores per Socket if desired. - The default value is taken from the selected snapshot in vCenter Server. - You can update this value again in the future using the Push Image function.	
Desktop Pool Settings		The following settings determine the desktop state, power status, and display protocol when a virtual machine is not in use.	
	State	- **Enabled**. After being created, the pool is enabled and ready for immediate use. - **Disabled**. After being created, the pool is deactivated and not available for use, and provisioning is stopped for the pool. Select this setting if you want other forms of baseline maintenance.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Connection Server restrictions	■ **No Restrictions**. The desktop pool can be accessed by any Connection Server instance. ■ **Restricted to these Tags**. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. You can restrict access to the pool to certain Connection Servers by clicking **Browse** and selecting one or more Connection Servers. **Note** If you intend to provide access to desktops through VMware Workspace ONE Access, and you configure Connection Server restrictions, the VMware Workspace ONE Access application might display desktops to users when those desktops are actually restricted. VMware Workspace ONE Access users will be unable to launch these desktops.	
	Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices. For more information, see "Configuring Shortcuts for Entitled Pools" in the *Horizon 8 Administration* document.	
	Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	
	Session Types	You can enable the VM Hosted Applications feature by selecting the supported session type for the desktop pool: ■ **Desktop**. Select this option to use the pool as a regular desktop pool. All the virtual machines in the pool can only be used to host desktops. ■ **Application**. Select this option to use all the virtual machines in the pool to host applications. ■ **Desktop and Application.** When this option is selected, the virtual machine in the pool can either host a regular desktop session or host an application session. The first connection to the particular virtual machine will determine the session type of the virtual machine. For more information about the VM Hosted Applications feature, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at https://techzone.vmware.com.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Remote Machine Power Policy	Determines the power state of instant clones after provisioning completes. This option is only available for dedicated pools. For descriptions of the power policy options, see Power Policies for Desktop Pools.	
	Log Off After Disconnect	■ **Immediately**. Users are logged off when they disconnect. ■ **Never**. Users are never logged off. ■ **After**. The time after which users are logged off when they disconnect. Type the duration in minutes. The logoff time applies to future disconnections. If a desktop session is already disconnected when you set a logoff time, the logoff duration for that user starts when you set the logoff time, not when the session was originally disconnected. For example, if you set this value to 5 minutes, and a session was disconnected 10 minutes earlier, Horizon 8 will log out that session 5 minutes after you set the value.	
	Bypass Session Timeout (Application and Desktop and Application session types)	Enable this setting to allow application sessions to run forever. When enabled, all the application sessions belonging to the desktop pool will never be disconnected automatically, neither when reaching the max session timeout nor when reaching the global idle timeout. This setting is available when you select session types **Application** and **Desktop or Application**. Application sessions that run forever are supported on Windows and Linux clients. You cannot enable this setting if any of the applications belonging to the desktop pool is part of Global Application Entitlement as local pools. This setting is not available for application pools in a cloud pod architecture environment. Application sessions that run forever are not supported for unauthenticated users. Do not enable this setting if the max session timeout value is set to **Never**. When you restart Connection Server, existing forever-running application sessions no longer run indefinitely.	
	Allow Users to Restart Machines	Specify whether users can reset the virtual machine or restart the virtual desktop. A reset operation resets the virtual machine without a graceful operating system restart. A restart operation restarts the virtual machine with a graceful operating system restart.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Refresh OS disk After Logoff	Select whether and when to refresh the OS disks. This option is available for dedicated assignment pools. ■ **Always**. The OS disk is refreshed every time the user logs off. Select this option to use App Volumes with dedicated instant clones. ■ **Every**. The OS disk is refreshed at regular intervals of a specified number of days. Enter the number of days. The number of days is counted from the last refresh, or from the initial provisioning if no refresh has occurred yet. For example, if the specified value is 3 days, and three days have passed since the last refresh, the desktop is refreshed after the user logs off. ■ **At**. The OS disk is refreshed when its current size reaches a specified percentage of its maximum allowable size. The maximum size of a instant clone's OS disk is the size of the replica's OS disk. Enter the percentage at which refresh operations occur. ■ **Never**. The OS disk is never refreshed.	
	Reclaim VM disk space	Determine whether to allow ESXi hosts to reclaim unused disk space on instant clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for instant-clone desktops. **Note** This setting is only applicable if you use a vSphere version earlier than 6.7 and if you use non-vSAN storage. For vSphere 6.7 and later, space reclamation is done automatically by vSphere and no additional steps are needed in Horizon 8.	
	Initiate reclamation when unused space on VM exceeds:	Enter the minimum amount of unused disk space, in gigabytes, that must accumulate on a instant-clone OS disk to trigger space reclamation. When the unused disk space exceeds this threshold, Horizon 8 initiates the operation that directs the ESXi host to reclaim space on the OS disk. This value is measured per virtual machine. The unused disk space must exceed the specified threshold on an individual virtual machine before Horizon 8 starts the space reclamation process on that machine. The default value is 1 GB. **Note** This setting is only applicable if you use a vSphere version earlier than 6.7 and if you use non-vSAN storage. For vSphere 6.7 and later, space reclamation is done automatically by vSphere and no additional steps are needed in Horizon 8.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Show Assigned Machine Name	Displays the host name of the assigned machine instead of the desktop pool display name when you log in to Horizon Client. If no machine is assigned to the user, then **Display Name (No Machine Assigned)** appears for the desktop pool when you log in to Horizon Client.	
	Show Machine Alias Name	Displays the machine alias name set for the assigned users of the machine instead of the desktop display name for the desktop pool in Horizon Client. Applies only to dedicated desktop entitlements. If no machine alias name is set but the **Show Assigned Machine Name** is set, then the machine host name appears for the desktop pool in Horizon Client. Otherwise, the desktop display name appears for the desktop pool in Horizon Client.	
	Allow Machine Name Selection	Enabling this option will allow a command line launch of Horizon Client to specify a machine name to connect to, for example for test or troubleshooting purposes. Applies only to floating desktop pools.	
	Empty session timeout (Applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select **Never**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select **Immediate**, the session logs you out or disconnects within 30 seconds. You can further reduce the time the session logs out or disconnects by editing a registry key on a Windows RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.	
	Pre-launch session timeout (Applications only)	Determines the timeout for the application session before the session is disconnected or logged off.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	When timeout occurs (Applications only)	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged off frees up resources, but opening an application takes longer. The default is **Disconnect**.	
	Allow user to initiate separate sessions from different client devices (Desktops only)	With this option selected, a user connecting to the same desktop pool from different client devices gets different desktop sessions. The user can only reconnect to an existing session from the same client device. When this setting is not selected, users are always reconnected to their existing session no matter which client device is used.	
	Used VM Policy	When an automated floating desktop pool is set to refresh or delete after logoff and if the desktop is not cleanly logged off, then the desktop goes into the **Already Used** state or the **Agent Disabled** state. This security feature prevents any previous session data from being available during the next login, but leaves the data intact to enable administrators to access the desktop and retrieve lost data or investigate the root cause of the reset. Administrators can then refresh or delete the desktop. Select from these options: ■ **Block Access**: The desktop is marked as **Already Used** and user access to the desktop is blocked. ■ **Allow without refresh**: The desktop is available without being refreshed. ■ **Auto refresh**: The desktop is automatically refreshed and users can access the desktop after the refresh operation is completed.	
Remote Display Setting		The following settings describe how the desktops are displayed to end users.	
	Default display protocol	Select the default display protocol. ■ For a Windows pool, the choices are **VMware Blast**, **PCoIP**, and **Microsoft RDP**. ■ For a Linux pool, **VMware Blast** is the only display protocol supported.	
	Allow users to choose protocol	Specify whether users can choose display protocols other than the default. This option is not applicable to Linux pools. ■ **Yes**. Allow users to choose a display protocol. ■ **No**. Do not allow users to choose a display protocol.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	3D Renderer	This field shows the type of 3D Render available for the instant-clone pool. This is not a selectable field. Depending on what you configured on the ESXi host and the golden image used for this pool, Horizon 8 will automatically display one of the following two options: ■ **NVIDIA GRID vGPU**. 3D rendering is enabled for NVIDIA GRID vGPU. ■ **Manage using vSphere Client**. The 3D Renderer option that you configured in vSphere Client. See Configure 3D Rendering Options for Instant-Clone Desktop Pools.	
	Allow Session Collaboration	Select **Enabled** to allow users of the desktop pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast protocol.	
Guest Customization			
	Domain	Select an Active Directory domain. The drop-down list shows the domains that you specify when you configure instant-clone domain administrators.	
	AD container	Specify the Active Directory container's relative distinguished name. For example: `CN=Computers`. Use the **Find** or **Browse** button to locate the Active Directory tree for the container. Click the Information icons next to the fields to get help using these options. ■ **Browse** - Returns a list of all containers in the AD. Use this option if you do not know the specific name of the container you are looking for. Note that this search may be slow when searching large AD environments. ■ **Find** - If you know the name of the container, use **Find** to perform a faster, more specific search. To list the child containers of the AD container or organizational unit, select **Subtree**, then **Find**.	
	Site Name	Select the Active Directory site for the pool. If the desktop network is at a different site than the Connection Server in a multi-site environment, you must select the correct Active Directory site for the pool. If you get an error, refer to KB Article 2147129 for more information. If you select Sysprep customization, it automatically selects sites for computer account creation and to perform domain join in multi-site environments. See Enabling Sysprep Guest Customization (without pre-created computer account).	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Allow Reuse of Existing Computer Accounts	Select this option to use existing computer accounts in Active Directory when the virtual machine names of new instant clones match the existing computer account names. See Allow Reuse of Existing Computer Accounts for Instant Clones. **Note** Recovery operations do not take this setting into consideration and always reuse the machine name.	
	Image Publish Computer Account	Instant-clone publishing requires an additional computer account in the same AD domain as the clones. Computer accounts are typically auto-created as needed. If you want to use pre-created computer accounts instead, also pre-create the additional computer account and specify its name here. This removes the need to delegate Create and Delete of computer objects to the provisioning account.	
	Use ClonePrep or a customization specification (Sysprep)	**Note** This option is not applicable to Linux pools. ClonePrep is the only customization method available for Linux machines. Choose whether to use ClonePrep or Sysprep to configure licensing, domain attachment, DHCP settings, and other properties on the machines. ClonePrep and Sysprep can run a customization script on instant-clone machines before they are powered off and after they are created or an image has been pushed to them. After you use ClonePrep or Sysprep when you create a pool, you can edit the customization type or spec name. Changes to the customization spec are not reflected on the pool until a new push image is scheduled, and the currently published image continues to use the old spec even if it has been edited or deleted. If push image fails, the pool continues using the old unedited spec. However, the pool settings continue to point to the new spec name if it has been changed. For more information about the differences between ClonePrep and Sysprep, see Choosing ClonePrep or Sysprep for Customizing Your Windows Virtual Desktops.	
	Power-Off Script Name	Specify the path name of a script to run on the desktop VMs and the script parameters before the VMs are powered off.	
	Power-Off Script Parameters	Example: p1 p2 p3	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (continued)

Option	Option	Description	Enter Your Value Here
	Post-Synchronization Script Name	Specify the path name of a script to run on the desktop VMs and the script parameters after the VMs are created.	
	Post-Synchronization Script Parameters	Example: p1 p2 p3	

This video explains how to configure network types in more detail.

(Configuring Network Types During Instant Clone Creation)

Create an Instant-Clone Desktop Pool

You can create an instant-clone floating desktop pool from a Windows or Linux virtual machine (VM) using the desktop pool wizard in Horizon Console. VMware Horizon 8 creates the instant-clone desktop VMs based on the settings that you specify when you create the pool.

Prerequisites

- Verify that the virtual switch that the instant-clone VMs connect to has enough ports to support the expected number of VMs. Each network card on a VM requires one port.
- Verify that the vCenter Server instance is added to Horizon Connection Server.
- Verify that you have the golden image ready. For more information, see Preparing a Windows Golden Image Virtual Machine for Instant Clones or Configure a Golden Image Linux VM for Instant Clones.

  Note You cannot create an instant-clone desktop pool from a VM template. You must first convert the VM template to a VM.

- Gather the configuration information for the pool. See Worksheet for Creating an Instant-Clone Desktop Pool.
- Verify that you have added an instant-clone domain administrator in Horizon Console. See *Horizon 8 Installation and Upgrade* on the VMware Horizon Documentation portal.
- Before creating an instant-clone desktop pool, take a snapshot of the golden image. You must shut down the golden image in vCenter Server before taking the snapshot. See "Take a Snapshot in the VMware Host Client" in *vSphere Single Host Management - VMware Host Client* on the VMware vSphere Documentation portal.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click **Add**.

3 Select **Automated Desktop Pool** and click **Next**.

4 Select **Instant Clones**, select the vCenter Server instance, and click **Next**.

5 Follow the prompts to create the pool.

   Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page by clicking the page name in the navigation pane.

   Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

   - If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
   - If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken.

   For more information, see the VMware Carbon Black Cloud Documentation. For best practices on using Carbon Black with VMware Horizon 8, see VMware Knowledge Base (KB) article 95512.

Results

In Horizon Console, you can view the desktop VMs as they are added to the pool by selecting **Inventory** > **Desktops**.

After you create the pool, do not delete the golden image or remove it from the vCenter Server inventory if the pool exists. If you remove the golden image VM from the vCenter Server inventory by mistake, you must add it back and then do a push image using the current image.

What to do next

Entitle users to access the pool. See "Entitling Users and Groups" in *Horizon 8 Administration* on the VMware Horizon Documentation portal.

Forensics Select Hold for Windows Instant-Clone Desktops

The purpose of the forensics select hold feature is to provide accurate and non-modified data for legal, security, and operational needs. The currently supported use case allows the live capture of data associated with a user’s desktop on a periodic basis when a user is put into a select hold for legal, incident response, or operational reasons. Putting a user on forensics select hold makes the user’s desktops temporarily persistent, thus avoiding refreshing or deletion (“re-imaging”) of the desktop and providing the administrator with the ability to access the user's desktop for investigative purposes with minimum impact to the user's experience.

This feature is supported for floating and dedicated Windows instant-clone desktop pools.

How the Forensics Select Hold Feature Works

- Role-based access control

  The forensics feature is controlled by the global privilege FORENSICS. The Super Administrator can assign this privilege to another administrator, who is known as the Forensics Administrator, but this privilege is not enabled for the Super Administrator by default. For more information, see "Global Privileges" in the *Horizon 8 Administration* document.

- Archival datastore

  The archival datastore is a mounted NFS or VMFS set globally in LDAP. Horizon 8 reads this setting from LDAP to determine where to place archived data. By default, the setting is to use the same datastore that the pool is on.

- Select hold workflow

  - Putting users on hold

    A hold can only be applied at an individual AD user level. When the Forensic Administrator puts a user on hold using the API, the following occur:

    - If the user is already using a VM, then the hold applies to the VM they are currently logged into, and to any other VMs assigned to the user.

    - When that user logs into a VM, Horizon 8 changes the state of the instant clone VM from stateless to stateful, but leaves the stateful VM in its original pool.

    - The user under hold continues to log back into the same VM and to see all the previous changes they made to their desktop. Horizon 8 does not alter the content of the VM in any way.

    - A status indicator in the administration console shows that the VM is in hold.

    - The VM is tagged as **Forensic** and protected in vCenter so that vCenter administrators do not accidentally alter or delete the VM.

  - During the hold period

    After a user is put on hold, the forensics team can access the stateful desktop for investigation as well as capture the live data on the fly. For this data capture, the forensics administrator has the following options.

    - Use the `Archive` API. The `Archive` API can work across multiple VMs and multiple users. You can only archive an individual VM when the user is not logged in. If user is logged in, then the archival command needs to be delayed until the user logs out.

      Archival operation is as follows:

      - The VM is shut down.

      - All disks are consolidated.

      - All snapshots are consolidated.

    - The VMDK file is copied to the selected archival location.
    - The VM is re-synced to the target image.
  - Use your own scripts or third party tools. In this case, you can choose whether to archive just hypervisor memory, just the VMDKs of the VMs, or both hypervisor memory and VMDKs.

    The `isHeldUser` environment variable indicates whether the user connecting to the session is a held user. Based on the value of this variable, you can trigger data collection scripts when a held user logs on to a desktop. A script can be triggered when the Script Host Service is running on the Connection Server VM. For more information, see Activate the VMware Horizon View Script Host Service in the *Horizon Remote Desktop Features and GPOs* document.

  Things to note during the hold period:

  - A held VM cannot be refreshed, recovered, removed, or put into maintenance mode. This applies only to the held VM, not to any other VMs in the same pool.
  - A pool containing held VMs cannot be deleted.
  - When the auto shrink capability of the pool is set, Horizon 8 prioritizes the held VM so that it is not lost.
  - When the instant clone pool needs to undergo pool refresh or patch update, there are two possible options:
    - When a pool containing held VMs needs to be refreshed and the archival datastore is not set, push image ignores the stateful VMs. This preserves the VMs under hold for forensics purposes, and the user continues to be directed to the persistent VM when they log in. These VMs must then be patched with separate tools like persistent VMs.
    - When a pool containing held VMs needs to be refreshed and the archival datastore is set, Horizon 8 first performs a push image on all the other VMs in the pool, then archives the held VMs. After the held VMs have been archived, Horizon 8 performs a normal push image process on them. The next time the held user logs back in, they get a pristine VM, which turns into a stateful VM, and the process repeats. Note that every time a patch operation happens, additional storage is required to copy and archive the stateful VM.
- Removing users from hold

  When the Forensics Administrator releases a user from hold using the API, the following occur.

  - Horizon 8 turns the VM back into a stateless VM.
  - The **Forensic** tag applied when the VM is put on hold is removed and the VM can be deleted from vCenter.

  - On the next user logoff, the VM is deleted and recreated from the golden image, thus reverting to a pristine state.

- Forensic operations in the Events database

  All operations, including granting of the FORENSICS privilege and holding/releasing users, are captured in the Events database. This can be used to notify any scripts that need to run.

Using APIs to Perform Forensics Select Hold Functions

You can use Horizon APIs to perform forensics select hold as described below. For each API, there is a link to its documentation on the VMware {code} website.

- Create Forensic Administrator Role and Assign a User

  a Create the custom Forensic Administrator role using the following API:

  ```
  /config/v1/roles
  ```

  Documentation for this API is found here.

  b Assign the custom Forensic Administrator role by following the instructions in "Create an Administrator in Horizon Console" in the *Horizon 8 Administration* guide.

- Designate a datastore for archiving

  To designate a datastore for archiving virtual disks and memory, use the following API:

  ```
  /config/v1/virtual-centers/{id}/action/mark-datastores-for-archival
  ```

  Documentation for this API is found here.

- Put User on Hold

  To put a user on hold, use the following API:

  ```
  /external/v1/ad-users-or-groups/action/hold
  ```

  The API returns the desktop ID, pool ID, and machine state for all desktops that are assigned to the held user. You can use this alert information to trigger scripted data collection. Documentation for this API is found here.

  In vCenter, the `ForensicHold` tag is applied to all the VMs used by held users.

- Archive the Virtual Disk and Memory of a VM

  To archive the virtual disk and memory of a VM, use the following API:

  ```
  /inventory/v1/machines/action/archive
  ```

  Documentation for this API is found here.

  - Archiving occurs when the user logs out of the held VM.

  - When VMs have been archived, they are shown inside the `Archive` folder on the archive datastore (as specified above in the API) in vCenter.
  - If a VM has more than one disk, then only the primary disk is archived. Multi-disk archival is not supported in this release.
- Release User From Hold

  To release a user from hold, use the following API:

  ```
  /external/v1/ad-users-or-groups/action/release-hold
  ```

  The API returns the desktop ID, pool ID, and machine state for all desktops that are assigned to the held user. You can use this alert information to trigger scripted data collection. Documentation for this API is found here.
- List Held Users

  To list held users, use the following API:

  ```
  /external/v1/ad-users-or-groups/held-users-or-groups
  ```

  Documentation for this API is found here.
- List Held Machines

  To produce a list of machines currently on hold, use the following API:

  ```
  /inventory/v3/machines
  ```

  Documentation for this API is found here.

  Note This API returns all machines. In the response, VMs on hold have the value `"held_machine": true`.

Configure Instant Clones with vSphere Virtual Machine Encryption

You can configure instant clones to use the vSphere Virtual Machine Encryption feature so that instant-clone desktops have the same encryption keys.

Prerequisites

- Verify that you are running VMware vSphere 7.0 or later.
- Create the Key Management Server (KMS) cluster with key management servers.
- To create a trust between KMS and vCenter Server, accept the self-signed certificate or create a certificate signed by a Certificate Authority (CA).

- In vSphere Client, create the `VMcrypt/VMEncryption` storage profile.

Note For details about the Virtual Machine Encryption feature in vSphere, see the *vSphere Security* document in the vSphere documentation portal.

Procedure

1 To configure instant clones that use the same encryption keys, use vSphere Client to create a golden image virtual machine (VM) with the `vmencrypt` storage policy.

  The `vmencrypt` storage policy applies only when the golden image VM does not have any snapshots. The clone inherits the golden image encryption state, including keys.

2 Take a snapshot of the golden image VM with the `vmencrypt` storage policy applied.

3 Create instant-clone desktops that point to the golden image VM with the `vmencrypt` storage policy applied so that all desktops have the same encryption keys.

  Note VM Encryption and Content Based Read Cache (CBRC) are not compatible. To use VM Encryption, you must disable CBRC globally by disabling View Storage Accelerator in Horizon Console by navigating to **Settings > Servers**.

Guest Customization for Windows Instant Clones in VMware Horizon 8

There are two options for customizing instant-clone Windows virtual machines (VMs) during the creation process: VMware ClonePrep and Microsoft Sysprep.

Note This page describes the guest customization options for Windows instant clones. For information on customizing Linux instant clones, see Using ClonePrep to Customize Linux Desktops.

ClonePrep is a VMware customization process run during instant clone deployment to personalize each desktop clone created from the parent image.

Sysprep is a Microsoft tool to deploy the configured operation system installation from a base image. The desktop can then be customized based on an answer script.

Guest Customization Options

ClonePrep and Sysprep ensure that all instant clones join an Active Directory domain. When you use ClonePrep, the clones have the same computer security identifiers (SIDs) as the golden image. If you need instant clones to have different SIDs from one another and from the golden image, use Sysprep. ClonePrep also preserves the globally unique identifiers (GUIDs) of applications, although some applications generate a new GUID during customization. For more guidance on the different clone types, see KB 2003797.

When you add an instant clone desktop pool, whether you are using ClonePrep or Sysprep, you can specify a script so that it runs immediately after a clone is created and another script to run before the clone is powered off.

- Running Scripts

  ClonePrep and Sysprep use the Windows `CreateProcess` API to run scripts. Your script can invoke any process that can be created with the `CreateProcess` API. For example, `cmd`, `vbscript`, `exe`, and batch-file processes work with the API.

  ClonePrep and Sysprep pass the path of the script as the second parameter to the `CreateProcess` API and sets the first parameter to `NULL`. For example, if the script path is `c:\myscript.cmd`, the call to `CreateProcess` is `CreateProcess(NULL,c:\myscript.cmd,...)`.

- Providing Paths to Scripts

  You can specify the scripts when you create or edit the desktop pool. The scripts must reside on the golden image. You cannot use a UNC path to a network share.

  If you use a scripting language that needs an interpreter to run the script, the script path must start with the interpreter executable. For example, instead of specifying `C:\script\myvb.vbs`, you must specify `C:\windows\system32\cscript.exe c:\script\myvb.vbs`.

  Important Put the customization scripts in a secure folder to prevent unauthorized access.

- Script Timeout Limit

  By default, ClonePrep and Sysprep terminate a script if the execution takes longer than 20 seconds. You can increase this timeout limit. For details, see Increase the Timeout Limit for ClonePrep Customization Scripts on a Windows Machine.

  Alternatively, you can specify a script that runs another script or process that takes a long time to run.

- Script Account

  ClonePrep and Sysprep run the scripts using the same account that the VMware Horizon Instant Clone Agent service uses. By default, this account is Local System. Do not change this login account. If you do, the clones can fail to start.

- Process Privileges

  For security reasons, certain Windows operating system privileges are removed from the VMware Horizon Instant Clone Agent process that runs customization scripts. The scripts cannot perform actions that require those privileges.

  The process that runs scripts do not have the following privileges:

  - SeCreateTokenPrivilege
  - SeTakeOwnershipPrivilege

  - SeSecurityPrivilege
  - SeSystemEnvironmentPrivilege
  - SeLoadDriverPrivilege
  - SeSystemtimePrivilege
  - SeUndockPrivilege
  - SeManageVolumePrivilege
  - SeLockMemoryPrivilege
  - SeIncreaseBasePriorityPrivilege
  - SeCreatePermanentPrivilege
  - SeDebugPrivilege
  - SeAuditPrivilege

- Script Logs

  ClonePrep and Sysprep write messages to a log file located in `C:\ProgramData\Vmware\VDM\Logs`.

Sysprep Guest Customization (with pre-created computer account)

You can provision an instant clone desktop pool with Microsoft Sysprep customization. In this workflow, Horizon will pre-create the computer accounts. You can also set pre-shutdown and post-synchronization scripts when using Sysprep customization.

Note the following information regarding Sysprep in Microsoft Windows guests.

- Microsoft Sysprep process might fail for certain Appx packages installed on the golden image VM. You must manually remove these Appx packages from the golden image VM for clone provisioning to complete. See the Microsoft support site.
- Sysprep can fail because there are Windows updates pending. To prevent this, run a Microsoft Windows update on the golden image VM and consider disabling the Microsoft Windows update service for instant clone. You can also check the Windows update page to confirm that there are no pending updates or errors displayed.
- By default, Sysprep generalize disables the built-in administrator account. If there is no other user account on the golden image VM, and if clone customization fails, users are not able to log in to the clone VM to collect debug information. When attempting to log in as local administrator, users will see a message on login screen saying 'Your account has been disabled. Please see your system administrator.' To resolve this issue, create new user accounts on the golden image VM following the instructions on the Microsoft support site.

- A vTPM device can be added to instant clones with ClonePrep or Microsoft Sysprep guest customization. Instant clone Smart Provisioning uses Mode B (clones created without parent VM) by default. However, if you are using a vTPM device on ESXi hosts with versions older than 7.0 update 3f then Smart Provisioning will select Mode A (clones created with parent VM). See KB 81026 for changing provisioning modes.

Sysprep Guest Customization (without pre-created computer account)

In this guest customization, Microsoft Sysprep will pre-create the computer accounts, not Horizon. If your AD environment is complex and consists of multiple sites and datacenters, you may run into provisioning issues described in this KB https://kb.vmware.com/s/article/2147129. Only a small portion of customers with multiple AD sites and datacenters have faced this issue. Use Sysprep guest customization without pre-created computer account to automatically select AD site for instant clone pool creation globally or at the pool level. Enabling the feature at the pool level allows you to test the new provisioning workflow on a test pool before enabling it globally for all pools using this workflow. See Enabling Sysprep Guest Customization (without pre-created computer account).

Install an SSL Certificate for VMware Blast on a Windows Machine

Installing an SSL certificate involves a post sysprep script/batch file and copying the certificate.

Use the post build configuration script `SetupComplete.cmd` to import the SSL certificate and configure the VMware HTML Access registry (applies to Windows 7 and later).

See https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/dd744268(v=ws.10).

Procedure

1 Copy the SSL certificate file to <path>.

2 Create a file `SetupComplete.cmd` in the < folder>. Create a folder called `Scripts` if it does not exist.

3 Add the following commands in the `SetupComplete.cmd` file.

4 If you have the root certificate and intermediate certificates in the certificate chain, then add the appropriate CertUtil commands in a batch file.

```
CertUtil  -importPFX -f  -p "<password>" "C:\<path>"
        reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t
REG_SZ /d "31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
del /F /Q "C:\<path>"
del /F /Q "%systemroot%\setup\scripts\SetupComplete.cmd"
```

5 Save the `SetupComplete.cmd` file. You can test the `SetupComplete.cmd` file on a test machine.

Enabling Sysprep Guest Customization (without pre-created computer account)

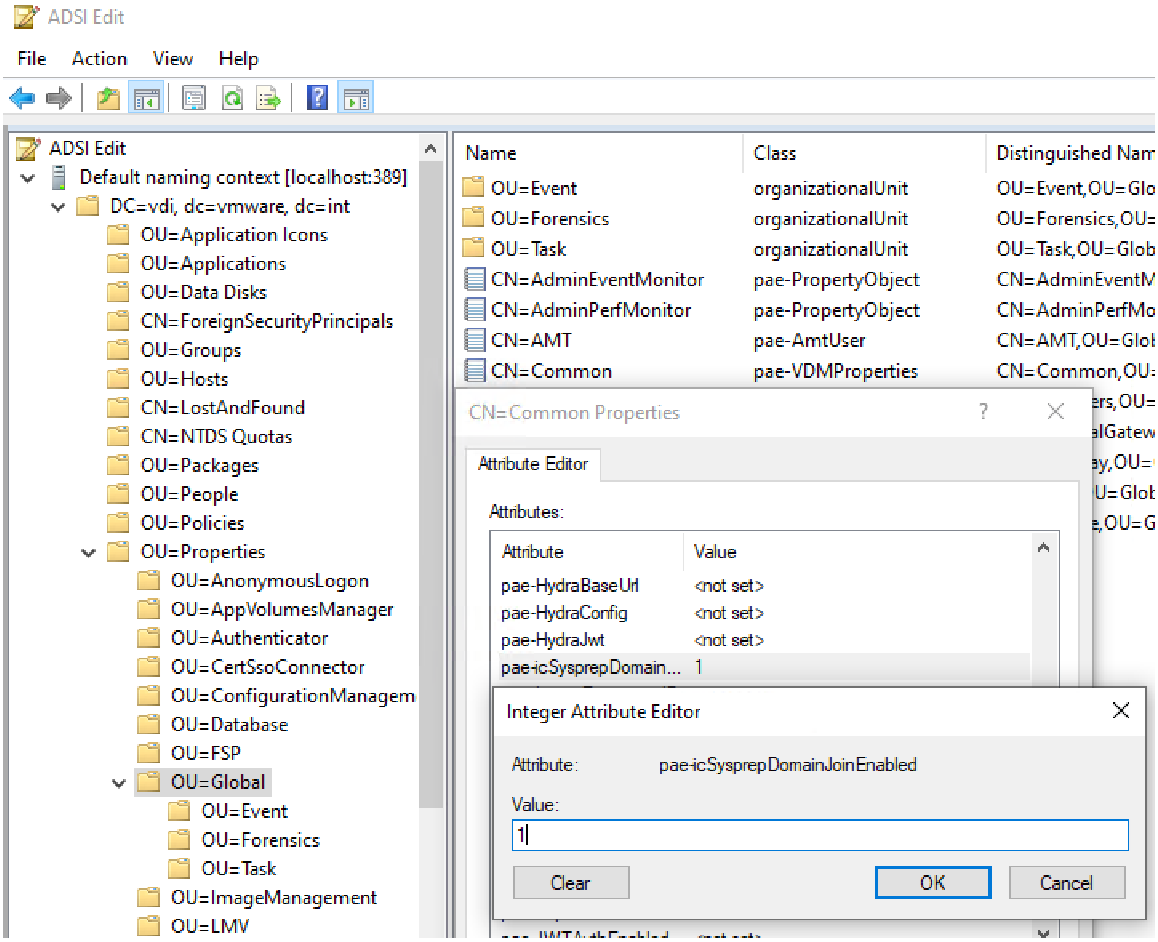
You can provision an instant clone desktop pool with Microsoft Sysprep without pre-created computer account customization to automatically select Active Directory sites.

To enable the feature globally or at a pool level, you use the ADAM database. Enabling the feature at the pool level allows you to test the new provisioning workflow on a test pool before enabling it globally for all sysprep pools.

Procedure

1 Set the attribute `pae-icSysprepDomainJoinEnabled` to the value of 1.

- To enable the feature globally: `CN=Common,OU=Global,OU=Properties,DC=vdi,DC=vmware,DC=int`



Name	Class	Distinguished Nam
OU=Event	organizationalUnit	OU=Event,OU=Glo
OU=Forensics	organizationalUnit	OU=Forensics,OU=
OU=Task	organizationalUnit	OU=Task,OU=Glob
CN=AdminEventMonitor	pae-PropertyObject	CN=AdminEventM
CN=AdminPerfMonitor	pae-PropertyObject	CN=AdminPerfMo
CN=AMT	pae-AmtUser	CN=AMT,OU=Glol
CN=Common	pae-VDMProperties	CN=Common,OU=

Attributes:

Attribute	Value
pae-HydraBaseUrl	<not set>
pae-HydraConfig	<not set>
pae-HydraJwt	<not set>
pae-icSysprepDomain...	1

Integer Attribute Editor

Attribute: pae-icSysprepDomainJoinEnabled

Value: 1

- To enable the feature at the pool level for existing pools: `CN=<PoolName>,OU=Server Groups,DC=vdi,DC=vmware,DC=int`

2 Create an instant clone desktop pool and follow the prompts. In the **Guest Customization** section, select **Use a Customization Specification (sysprep)**.

   The **Site Name** field is not available.

3 Create a VM Customization Spec in vCenter.

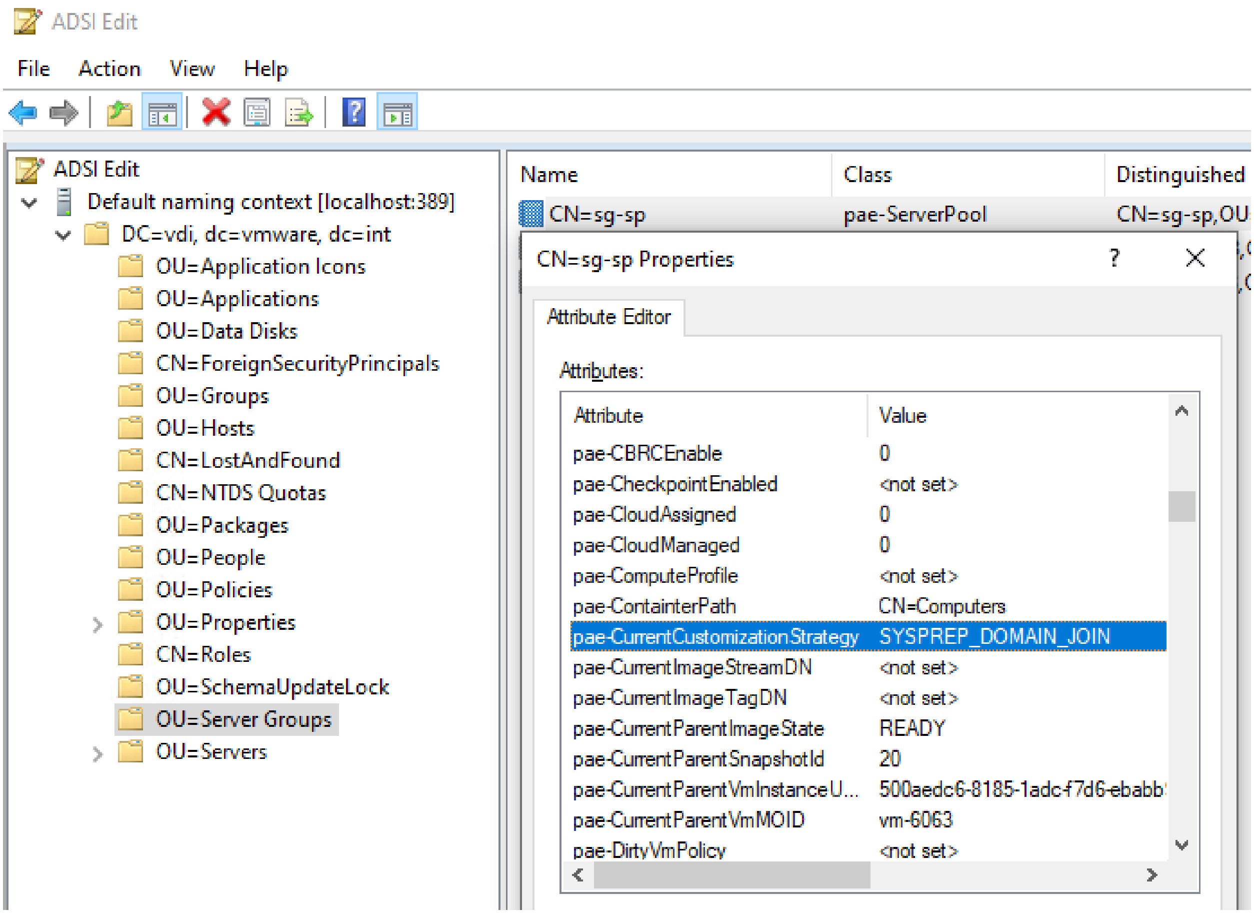
   The **Workgroup or Domain** field can be the default value. In **Administrator Password** if a password is specified, the password for the Administrator account is set to that value and the administrator account is disabled.

4 Complete the new instant clone sysprep pool creation.

5 Perform a push image on existing sysprep pools for changes to take effect.

Results

After a pool is provisioned with the new workflow, the `pae-CurrentCustomizationStrategy` is set to`SYSPREP_DOMAIN_JOIN` in the `pae-ServerPool` object in the ADAM database.



Name	Class	Distinguished
CN=sg-sp	pae-ServerPool	CN=sg-sp,OU

Attribute	Value
pae-CBRCEnable	0
pae-CheckpointEnabled	<not set>
pae-CloudAssigned	0
pae-CloudManaged	0
pae-ComputeProfile	<not set>
pae-ContainterPath	CN=Computers
pae-CurrentCustomizationStrategy	SYSPREP_DOMAIN_JOIN
pae-CurrentImageStreamDN	<not set>
pae-CurrentImageTagDN	<not set>
pae-CurrentParentImageState	READY
pae-CurrentParentSnapshotId	20
pae-CurrentParentVmInstanceU...	500aedc6-8185-1adc-f7d6-ebabb
pae-CurrentParentVmMOID	vm-6063
pae-DirtyVmPolicy	<not set>

Enabling VBS and vTPM for a Windows Instant-Clone Desktop Pool

You can enable Microsoft VBS and add a Virtual Trusted Platform Module (vTPM) device to Windows instant-clone desktop pools.

Note vTPM can be enabled for desktop pools without enabling VBS. Additionally, although Microsoft recommends a vTPM when enabling VBS, it is not a requirement.

To set up the Key Management Server cluster, which is a prerequisite, see "Set up the Key Management Server Cluster" in the *vSphere Security* document in the vSphere documentation..

For compatibility requirements, see "Securing Virtual Machines with Virtual Trusted Platform Module" in the *vSphere Security* document in the vSphere documentation.

To enable VBS, the golden image used must have VBS enabled when creating the VM and the local security policy set to "enable VBS" inside the guest operating system.

A vTPM device can be added to instant clones with ClonePrep or Microsoft Sysprep guest customization. Instant clone Smart Provisioning uses Mode B (clones created without parent VM) by default. However, if you are using a vTPM device on ESXi hosts with versions older than 7.0 update 3f then Smart Provisioning will select Mode A (clones created with parent VM). See https://kb.vmware.com/s/article/81026 for changing provisioning modes.

You can also select or deselect the option to add or remove a vTPM during a push-image operation.

Configure 3D Rendering Options for Instant-Clone Desktop Pools

When you create or edit a desktop pool of virtual machines, you can configure 3D graphics rendering for your desktops. You must configure 3D settings in ESXi hosts and in the golden image in vSphere Client.

VMware Horizon 8 does not directly control settings for 3D rendering of an instant-clone pool as it does with full-clone virtual machines. You must configure 3D settings in the ESXi hosts, and then in your golden image using the vSphere Client. Instant-clone virtual machines will inherit those settings from the golden image. Horizon Console will display some of the settings you configured, but you cannot edit or interact with those settings.

End users can take advantage of 3D applications for design, modeling, and multimedia, which typically require GPU hardware to perform well. For users that do not require physical GPU, a software option provides graphics enhancements that can support less demanding applications. Instant clones support the following 3D graphics options:

NVIDIA GRID vGPU (shared GPU hardware acceleration)

This feature allows a physical GPU on an ESXi host to be shared among virtual machines. This feature offers flexible hardware-accelerated 3D profiles ranging from lightweight 3D task workers to high-end workstation graphics power users.

Soft 3D - for Windows instant clones only

Software-accelerated graphics allow you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical GPU. For users that do not require a physical GPU, a software option provides graphics enhancements that can support less demanding applications, such as Windows AERO, Microsoft Office, and Google Earth.

Virtual Shared Graphics Acceleration (vSGA) - for Windows instant clones only

This feature allows multiple virtual machines to share the physical GPUs on ESXi hosts and is suitable for mid-range 3D design, modeling, and multimedia applications.

Note Instant clones do not support Virtual Directed Graphics Acceleration (vDGA) or AMD MxGPU.

In some cases, if an application such as a video game or 3D benchmark forces the desktop to display in full screen resolution, the desktop session can be disconnected. Possible workarounds include setting the application to run in Windows mode or matching the Horizon 8 session desktop resolution to the default resolution expected by the application.

Note that this guide does not provide complete information for configuring virtual machines and ESXi hosts for vSGA or NVIDIA GRID vGPU. These tasks must be done with vSphere Client before you attempt to create desktop pools in Horizon Console.

To disable 3D rendering in the vSphere Client, deselect **Enable 3D Support** for the golden image using the vSphere Client. See Configuring 3D Graphics in the *vSphere Virtual Machine Administration* guide.

Enable NVIDIA GRID vGPU for Instant-Clone Pools

You can configure NVIDIA GRID vGPU in ESXi hosts and in the golden image in vSphere Client.

The ESXi host assigns GPU hardware resources to virtual machines on a first-come, first-served basis as virtual machines are created. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is the **best performance** mode. If you would rather have the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU, you can use the **GPU consolidation** mode. You can configure this mode in vCenter Server for each ESXi host that has vGPU installed. For more information, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/55049.

If you are only using a single vGPU profile per vSphere cluster, set the GPU assignment policy for all GPU hosts within the cluster to the **best performance** mode in order to maximize performance. In this case, you can also have instant-clone pools and full-clone pools that use the same vGPU profile in the same vSphere cluster.

You can have a cluster with some GPU enabled hosts and some non-GPU enabled hosts.

Note The following considerations apply to the vMotion of vGPU Virtual Machines feature.

- vMotion of vGPU Virtual Machines is supported starting with vSphere 6.7. See here for details on how to configure this and more information.
- vSphere Distributed Resource Scheduler (DRS) in vSphere 6.7 Update 1 and later supports initial placement of vGPU VMs without load balancing support.
- DRS in vSphere 6.7 or vSphere 7.0 versions earlier than vSphere 7.0 U3f will not automatically vMotion vGPU VMs when ESXi hosts are placed in maintenance mode. An administrator is required to manually initiate vMotion of vGPU VMs in order to allow ESXi hosts to enter maintenance mode.
- DRS in vSphere 7.0 U3f and later can be configured to allow automatic vMotion when hosts are placed in maintenance mode. See https://kb.vmware.com/s/article/88271 for instructions. DRS load balancing remains unsupported for vGPU VMs.

NVIDIA GRID vGPU has these potential constraints:

- RDP is not supported.
- The virtual machines must be hardware version 11 or later.
- Horizon 8 does support creating a vGPU instant-clone pool using a cluster with some vGPU enabled hosts and non-vGPU enabled hosts, and will just ignore the non-vGPU enabled hosts when creating the pool. You can not use vMotion to move an instant-clone from a GPU-enabled ESXi host to an ESXi host that does not have GPU hardware configured.

To enable an instant-clone pool to use NVIDIA GRID vGPU:

Procedure

1. Install NVIDIA GRID vGPU in the physical ESXi hosts.
2. In vCenter Server hardware graphics configuration, select the Host Graphics tab, and in **Edit Host Graphics Settings**, select **Shared Direct**.

   The ESXi host uses the NVIDIA GRID card for vGPU.
3. Prepare a golden image with NVIDIA GRID vGPU configured, including selecting the vGPU profile you want to use.
4. Take a snapshot of the golden image.
5. In Horizon Console, when you create an instant-clone pool, select this golden image and snapshot.

Results

Horizon 8 automatically displays **NVIDIA GRID vGPU** in the 3D Render field. Horizon 8 also displays the vGPU profile you chose in the golden image. Instant clones inherit the settings configured in the vSphere Client for the golden image.

The vGPU profile cannot be edited from Horizon Console during the instant-clone pool creation process, To edit the vGPU profile for a pool once the pool has been created, you can create a new image with the updated vGPU profile, take a snapshot, and then do a push-image operation. See Patching an Instant-Clone Desktop Pool .

Enable Soft 3D for Windows Instant-Clone Pools

When you enable Soft 3D, the ESXi host uses software 3D graphics rendering.

If a GPU graphics card is installed on the ESXi host, this pool will not use it. Horizon 8 does not control or configure 3D rendering settings because they are all set in the golden image VM using vSphere Client.

To enable Soft 3D in the golden image VM:

Procedure

1. In the vSphere Client, 3D Render field, select **Software**.
2. Configure **Number of displays**, **Total video memory**, and **3D memory** for the instant-clones to inherit from the golden image.
3. Take a snapshot of the golden image.
4. In Horizon Console, when you create an instant-clone pool, select this golden image and snapshot.

Results

Horizon 8 automatically displays **Manage Using vSphere Client** in the 3D Render field. Instant-clones inherit the settings configured in the vSphere Client for the golden image.

Enable vSGA for Windows Instant-Clone Pools

When you enable vSGA, the ESXi host uses hardware 3D rendering, provided that GPU resources are available on the ESXi hosts.

To enable vSGA, install GPU graphics cards and the associated vSphere Installation Bundles (VIBs) on the ESXi hosts. For a list of supported GPU hardware, see the VMware Hardware Compatibility List.

Procedure

1. In vCenter Server hardware graphics configuration, select the Host Graphics tab, and in **Edit Host Graphics Settings**, select **Shared**.

   ESXi host uses the GPU hardware for vSGA mode.

2. In the vSphere Client, configure the golden image 3D Render field with these two options.

   - Select **Hardware**. Select this option if you only want to use vSGA hardware 3D render. Potential constraints when selecting this option are that when all GPU resources on an ESXi host are reserved, Horizon 8 cannot create another virtual machine for the next user, and the user will receive an error message. You must manage the allocation of GPU resources and the use of vMotion to ensure that resources are available for your desktops. vMotion is supported for vSGA-enabled hosts, but only across those hosts with GPU hardware. When you configure hardware-based 3D rendering, you can examine the GPU resources that are allocated to each virtual machine on an ESXi host. For details, see Examining GPU Resources on an ESXi Host.

  - Select **Automatic**. If you select this option, vSGA-enabled virtual machines can switch dynamically between software and hardware 3D rendering. Automatic uses hardware acceleration if there is a capable and available hardware GPU in the ESXi host. If a hardware GPU is not available, the virtual machine uses software 3D rendering for any 3D tasks. This option ensures that some type of 3D rendering takes place even when GPU resources are completely reserved.

3. Configure **Number of displays**, **Total video memory**, and **3D memory** for the instant-clones to inherit from the golden image.
4. Take a snapshot of the golden image.
5. In Horizon Console, when you create an instant-clone pool, select this golden image and snapshot.

Results

Horizon 8 automatically displays **Manage Using vSphere Client** in the 3D Render field. Instant-clones inherit the settings configured in the vSphere Client for the golden image.

Configure Monitors and Screen Resolution for Instant Clones

You can specify the number of monitors and resolution for your instant-clone desktop pool in vSphere Client by setting those parameters in the golden image and taking a snapshot.

The required vRAM size is calculated based on your specifications. Select the snapshot of the golden image to use for the pool. The snapshot lists the following details:

- Number of monitors
- VRAM size
- Resolution

The instant-clone desktop pool created is based on the golden image snapshot and inherits those memory settings. You cannot configure these settings in Horizon Console for instant clones.

For more information about configuring video memory settings in vSphere Client, see the *vSphere Single Host Management* document on the VMware vSphere Documentation portal.

For more information about changing the resolution for your instant-clone desktop pool, see the VMware Knowledge Base (KB) article http://kb.vmware.com/kb/2151745.

Allow Reuse of Existing Computer Accounts for Instant Clones

You can configure instant clones to reuse existing Active Directory (AD) computer account names.

Enable this option if you have a limited number of computer accounts to use. When an instant clone is created, if an existing AD computer account name matches the instant-clone virtual machine name, VMware Horizon 8 uses the existing computer account after resetting the password. Otherwise, a new computer account is created. When the instant clone is deleted, Horizon 8 does not delete the corresponding computer accounts. The existing computer accounts must be located in the Active Directory container that you specify with the AD container setting.

When this option is turned off, a new AD computer account is created when Horizon 8 creates an instant clone. When the instant clone is deleted, Horizon 8 deletes the corresponding computer account. If an existing computer account matches the instant-clone virtual machine name, Horizon 8 reuses the existing computer account after resetting the password.

This option is turned off by default.

If you have enabled this option, it is important to follow the steps in *Create a User Account for Instant Clone Operations* in the Horizon Installation and Upgrade guide to create an instant clone user account with correct permissions. Using a user account with insufficient permissions might result in domain join failure if you applied Microsoft security update KB5020276 as described in KB 92214.

Manually Customizing Machines in an Automated Desktop Pool

After you create an automated pool, you can customize particular machines without reassigning ownership. By starting the machines in maintenance mode, you can modify and test the machines before you release them to users.

Maintenance mode prevents users from accessing their desktops. If you start machines in maintenance mode, VMware Horizon 8 places each machine in maintenance mode when the machine is created. In a dedicated-assignment pool of full virtual machines, you can use maintenance mode to log in to a machine without having to reassign ownership to your own administrator account. When you finish the customization, you do not have to return ownership to the user assigned to the machine.

To perform the same customization on all machines in an automated pool, customize the virtual machine you prepare as a template. Horizon 8 deploys your customization to all the machines.

Note You can start machines in maintenance mode if you manually specify machine names for the pool, not if you name machines by providing a naming pattern.

Customize Machines by Placing Them in Maintenance Mode After Pool Creation

After an automated desktop pool is created, you can customize, modify, or test individual machines by placing them in maintenance mode. When a machine is in maintenance mode, users cannot access the virtual machine desktop.

You place existing machines in maintenance mode one at a time. You can remove multiple machines from maintenance mode in one operation.

When you create a desktop pool, you can start all the machines in the pool in maintenance mode if you specify machine names manually.

Procedure

1. In Horizon Console, select **Inventory > Desktops**.
2. Click the link for the pool.
3. Select the **Machines** tab.
4. Select a machine.
5. Select **Enter Maintenance Mode** from the **More Commands** drop-down menu.
6. Customize, modify, or test the virtual machine desktop.
7. Repeat steps to select a machine and customize, modify, or test the virtual machine desktop.
8. Select the customized machines and select **Exit Maintenance Mode** from the **More Commands** drop-down menu.

Results

The modified virtual machine desktops are available to users.

Customize Machines by Starting Them in Maintenance Mode During Pool Creation

You can customize individual machines after an automated pool is created by starting the machines in maintenance mode.

Procedure

1. In Horizon Console, begin creating an automated desktop pool by starting the **Add Pool** wizard.
2. On the Provisioning Settings page, select **Specify names manually**.
3. Select **Start machines in maintenance mode**.
4. Complete the **Add Pool** wizard to finish creating the desktop pool.

5 In vCenter Server, log in, customize, and test the individual virtual machines.

   You can customize Windows machines manually or by using standard Windows systems-management software such as Altiris, SMS, LanDesk, or BMC.

6 In Horizon Console, select **Inventory > Machines**.

7 Select specific machines to release to your users.

8 Click **More Commands > Exit Maintenance Mode**.

What to do next

Notify your users that they can log in to their desktops.

Patching an Instant-Clone Desktop Pool

To patch a pool of instant-clone desktops, you can use the push-image operation for a rolling patching process with zero downtime.

The image you used to create a pool is the default image. By default, all patching operations use this image to update all machines in the pool. Depending on how you want the golden image to be managed, you can change the golden image and snapshot source in your pool from vCenter to Image Catalog or reverse. For more information on the Image Management Service, see the *Managing Horizon Images from the Cloud* document.

You can optionally publish a secondary image, which you can use to update a subset of the machines in the pool while leaving the rest unchanged. Find out more in Selective Patching of Virtual Machines.

When you are using the default image, the workflow for the patching process is as follows:

- Prepare a new golden image and snapshot based on the updated operating system image or applications.
- Schedule a push-image operation with the updated golden image and snapshot. When the push-image operation starts, VMware Horizon 8 deletes old instant-clone desktops that are unused and quickly creates new instant clones based on the new image. The new clones are ready for users to log in.
- Old instant-clone desktops that are in-use remain undisturbed. When the user logs out, Horizon 8 deletes the old instant clone and recreates a new instant clone based on the updated image. The new instant clone is ready for the next user to log in.
- Once all the users have logged out, Horizon 8 patches the entire pool.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click the pool ID.

3 On the **Summary** tab, click **Maintain > Schedule**.

The **Schedule Push Image** window opens.

4 On the Image step, select the snapshot to use. The default image for the pool is already selected. If the image source is Image Catalog, please select stream and marker.

Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

- If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
- If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken.

For more information, see the VMware Carbon Black Cloud Documentation. For best practices on using Carbon Black with VMware Horizon 8, see VMware Knowledge Base (KB) article 95512.

5 On the Schedule step, select the **Schedule image push** option.

You can schedule the task to start immediately or sometime in the future. For clones with user sessions, you can specify whether to force the users to log out or to wait. When the users log out, Horizon 8 recreates the clones.

6 On the Ready to Complete step, click **Finish**.

Results

When you schedule this operation, publishing of the new image starts immediately. The pool update starts at the time that you specify in the **Schedule Push Image** wizard.

Selective Patching of Virtual Machines

Consider a scenario where before updating an entire pool with a new image, you would like to first try it out on a subset of the pool so that you know that the new image works, and users are able to login. This feature gives administrators an option to either update the entire pool or specify a set of virtual machines (VMs) to update. It allows a single desktop pool to support two images at the same time.

Patch Selected VMs In the Pool Using a Secondary Image

When you are using a secondary image, the workflow for the patching process is as follows:

- Prepare a secondary golden image and snapshot based on the updated operating system image or applications.

- Perform a push-image operation with the secondary golden image and snapshot. You have two options for this operation:
  - Publish the secondary image without immediately applying it to any machines in the pool.
  - Publish the secondary image and immediately apply it to selected machines in the pool.
- After you have published the secondary image, options are enabled to apply either of the images to selected machines without using the **Schedule Push Image** process.

To patch selected VMs in the pool using the secondary image, perform the following steps.

1. In Horizon Console, select **Inventory > Desktops**
2. Click the pool ID.
3. On the **Summary** tab, click **Maintain > Schedule**.

   The **Schedule Push Image** window opens.
4. On the Image step, select the secondary image and snapshot to use.

   Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

   - If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
   - If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken.

   For more information, see the VMware Carbon Black Cloud Documentation. For best practices on using Carbon Black with VMware Horizon 8, see VMware Knowledge Base (KB) article 95512.
5. On the Schedule step, select the **Publish Secondary image** option.

   To immediately apply the secondary image to selected machines, select the **Push to specific machines** check box and then select machines from the list.
6. On the Ready to Complete step, click **Finish**.

Switching Between the Default and Secondary Image

After you have published the secondary image, options are enabled on the **Machines (Instant Clone Details)** tab to apply either of the images to selected machines.

- To apply the secondary image, select the machines on the **Machines (Instant Clone Details)** page and then select **More Commands > Apply Secondary Image**.

  Note The secondary image applies only when the pool is selected for **All Machines up-front** and not when **Machines on Demand** is selected.

- To apply the default image, select the machines on the **Machines (Instant Clone Details)** page and then select **More Commands > Apply Default Image**.

Promote or Cancel the Secondary Image

If the new image meets your acceptance criteria, you can promote this secondary image to be your default image. Otherwise, you can cancel the secondary image and the default image will get applied to the desktop pool.

- There is an option on the **Summary** tab to promote the secondary image. This causes the secondary image to become the new default image on the pool and applies it to all the machines in the pool. To promote the secondary image, select **Maintain > Promote Secondary Image**.
- To cancel the secondary image, select **Maintain > Cancel** on the **Summary** tab.
  - If the pool is set to refresh on logoff, the desktops that are currently on the secondary image will revert to the default image once the user logs off.
  - If the pool is not set to refresh on logoff, the desktops on the secondary image remain on it unless a recover, delete, or refresh is performed on the desktop.

Monitor a Push-Image Operation

You can monitor the progress of a push-image operation on an instant-clone desktop pool.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click the pool ID.

The **Summary** tab shows the current image and pending image information, including any push-image error messages.

3 Click the **Tasks** tab.

The list of tasks that are associated with the push-image operation appears.

Reschedule or Cancel a Push-Image Operation

You can reschedule or cancel a push-image operation on an instant-clone desktop pool.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click the pool ID.

The **Summary** tab shows the current image and pending image information.

3 Select **Maintain > Reschedule** or **Maintain > Cancel**.

4 Follow the prompts.

Results

If you reschedule or cancel the push-image operation while clone creation is in progress, the clones that have the new image remain in the pool and the pool has a mix of clones, some with the new image and the others with the old image. To ensure that all the clones have the same image, you can remove all the clones. VMware Horizon 8 recreates the clones with the same image.

Perform Maintenance on Instant-Clone Hosts

You can perform maintenance on hosts where instant clones reside by putting the ESXi hosts into maintenance mode. You use vSphere Client to put the ESXi host into maintenance mode.

In most cases, using instant clones does not change your operational flow of how you perform ESXi host maintenance tasks. VMware Horizon 8 will automatically delete the instant clone parentVMs to allow the ESXi host to go into maintenance mode. When you use VMware Update Manager, an extra step is required.

If you use VMware Update Manager to update your ESXi hosts, you must delete or disable the instant clone parentVM before VMware Update Manager can successfully update the ESXi hosts. If you use an older version of Horizon, you must manually delete the instant clone parentVM on all the ESXi hosts by using the instant-clone utilities. To use the instant-clone utilities, see Instant-Clone Maintenance Utilities.

Starting with Horizon 8 version 2006, you can globally deactivate all of the instant clone parentVMs in a vCenter Server so that VMware Update Manager can update the ESXi hosts in that vCenter Server. If you deactivate the parentVM setting for a vCenter Server, Horizon 8 will automatically delete all the parentVMs on every single host in that vCenter Server, so that the hosts can go into maintenance mode without any manual intervention. Deleting the parentVM does not impact the operations of instant clones as Horizon 8 can create instant clones with or without parentVMs.

To selectively disable parentVMs for certain clusters only rather than the entire vCenter Server, see the KB article 80369. If you leave the parentVM setting for the vCenter Server deactivated, any new instant clones are then provisioned without parentVMs. If you want Horizon 8 to use parentVMs when creating instant clones, then you can re-enable the parentVM setting for the vCenter Server after VMware Update Manager completes host maintenance. You must deactivate the parentVM for the vCenter Server before every update event.

Note If you use VMware Update Manager, keep the instant clone parentVMs deactivated for your vCenter Server to simplify your ESXi maintenance.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. Select the server from the list, click **More** and select **Disable ParentVMs**.
3. Log in to vSphere Client.

4 Select the ESXi host that you want to put into maintenance and click **Maintenance Mode > Enter Maintenance Mode**.

MAC Address Behavior for Instant-clone Operations

The following table describes the MAC address behavior that results when an instant-clone desktop goes through different operations.

Operation	Floating Instant Clones	Dedicated Instant Clones with Refresh on Each User Logout
When a user logs out	■ Mode A: Creates a new clone and then destroys the old clone after certain information like MAC address is copied over. ■ Mode B: VMware Horizon 8 refreshes by reverting to the snapshot.	■ Mode A: Creates a new clone and then destroys the old clone after certain information like MAC address is copied over. ■ Mode B: Horizon 8 refreshes by reverting to the snapshot.
Computer name after user logs out / instant-clone refresh	■ New computer name assigned to user after logout	■ Same computer name assigned to user after logout
MAC address after user logs out / instant-clone refresh	■ The same MAC address is preserved on the VM where logout occurred. ■ When a user logs in again, they receive a new VM with a new MAC address since they are working with a floating pool.	■ The same MAC address is preserved on the VM where logout occurred.
On push image	■ Deletes old instant clone and creates a new one. ■ New computer name/VM is assigned to user after logout since they are working with a floating pool and assignment is random by nature. ■ VM is assigned a new MAC address.	■ Deletes old instant clone and creates a new one. ■ Same computer name/VM is assigned to user after logout. ■ Same MAC address is preserved on the VM.
On VM removal	■ Clone is deleted and recreated with a new MAC address.	■ Clone is deleted and recreated with a new MAC address.

Instant-Clone Maintenance Utilities

On the Connection Server are three utilities that you can use for the maintenance of instant-clone virtual machines (VMs) in vCenter Server and the clusters that the VMs are in.

The utilities are `IcMaint.cmd`, `IcUnprotect.cmd`, and `IcCleanup.cmd` and are located in `C:\Program Files\VMware\VMware View\Server\tools\bin`.

IcMaint.cmd

Typically, when you put the ESXi host into maintenance mode, VMware Horizon 8 automatically deletes the parent VM so that the host can go into maintenance mode without any manual intervention.

However, you can use this command to delete cp-parent VMs. The host is not automatically put into maintenance mode. To perform maintenance on the host, the vCenter Server administrator must manually put the host into maintenance mode.

Syntax:

```
IcMaint.cmd -vc hostname_or_IP_address -uid user_ID -hostName ESXi_hostname -maintenance ON|OFF
```

Parameters:

- `-vc` *host name or IP address of vCenter Server*
- `-uid` *vCenter Server user ID*
- `-hostname` *ESXi host name*
- `-maintenance` `ON|OFF`

  This parameter specifies whether the host is available for hosting the golden image VM.

  After the command is run on the host, the InstantClone.Maintenance annotation value is set to 1 and the golden image VMs are deleted. After the golden image VMs are deleted, the InstantClone.Maintenance annotation value is set to 2 and no more golden image VMs are created on the host. When you run this command again with `–maintenance` `OFF`, the InstantClone.Maintenance annotation value is cleared for the host to become available for hosting golden image VMs.

All the parameters are required.

IcUnprotect.cmd

After ClonePrep creates folders and VMs, you can use this utility to unprotect folders and VMs, delete VMs, and detect VMs whose golden image or snapshot is deleted. ClonePrep is the mechanism that customizes instant clones during the creation process.

Note An internal service for instant clones that runs during instant clone operations, detects if any internal folders need to be reprotected. If these folders are not empty then the service automatically protects the folders again.

Syntax:

```
IcUnprotect.cmd -vc hostname_or_IP_address -uid user_ID [-includeFolders][-skipCertVeri]
```

Parameters:

- `-action`

  You can use the following options for this parameter:

  - `unprotect`. Unprotect internal VMs.
  - `delete`. Delete internal VMs.
  - `detect`. Detect and list internal VMs whose golden image or snapshot is deleted.

  If you don't specify the `-action` parameter, the internal VMs are unprotected by default.

- `-vc` *host name or IP address of vCenter Server*
- `-uid` *vCenter Server user ID*
- `-clientId` *instant-clone client ID* (Optional)

  If `clientId` is not specified, protection is removed from all ClonePrep VMs in all data centers.

- `-domain` *domain name* (Optional)

  You can use multiple domain names separated by comma and no space.

- `-host` *host name* (Optional)

  You can use multiple host names separated by comma and no space.

- `-datastore` *datastore name* (Optional)

  You can use multiple datastore names separated by comma and no space.

- `-vmName` *VM name* (Optional)

  You can use multiple VM names separated by comma and no space.

- `-vmType` *internal VM type* (Optional)

  You can use multiple VM types separated by comma and no space. You can use template, replica, parent as options for this parameter.

- `-includeFolders` *include folders*

  This parameter unprotects the folders in addition to the VMs.

- `-skipCertVeri` *skip certification verification*

  `IcUnprotect.cmd` enforces host name verification. You must enter the correct host name of the vCenter Server instead of its IP address when you specify the command parameters. To disable host name verification and use the IP address of vCenter Server instead, use `-skipCertVeri`.

Specify the following parameters to delete all parent VMs in vCenter Server:

```
IcUnprotect -action delete -vc <IP address of vCenter Server> -uid <vCenter Server user ID>
-clientId <instant clone client ID> -host <hostname 1>,<hostname 2> -vmType parent
```

Specify the following parameters to delete specific parent VMs in vCenter Server:

```
IcUnprotect -action delete -vc <IP address of vCenter Server> -uid <vCenter Server user ID>
-clientId <instant clone client ID> -host <hostname 1>,<hostname 2> -vmType parent -vmName
<parent VM name 1>,< parent VM name 2>
```

IcCleanup.cmd

You can use this utility to unprotect and delete some or all of the internal VMs created by instant clones. This utility also provides a list command to group internal VMs into the hierarchical structure according to their golden VM and the snapshot used to create the instant clone pool. The list command has a detect option which only reveals the internal VM groups with priming tag or snapshot missing. You can then unprotect and delete a specific group or all of these groups. You can also output all the groups into a disk file for future reference.

Syntax:

```
iccleanup.cmd -vc vcName -uid userId [-skipCertVeri] [-clientId clientUuid]
```

Parameters:

- `-vc` *host name or IP address of vCenter Server*
- `-uid` *vCenter Server user ID*
- `-skipCertVeri` *Skip the vCenter Server certificate verification* (Optional)
- `-clientId` *Client UUID, the unique ID for the server cluster made up of Connection Server and one or more replica servers.* (Optional)

  Note To find the client UUID, log into Connection Server or any of the replica servers, run `ADSI Edit`. In **DC=vdi, dc=vmware, dc=int > OU=Properties > OU=Global > CN=Common**, find the value for `pae-GUID`, which is the value for the client UUID. If you do not specify the client UUID, the cleanup tool will deal with all the internal VMs. If you specify the client UUID, the cleanup tool will deal with only the internal VMs that belong to that particular client UUID.

Commands:

- `list` List some or all the internal VMs and present them in a hierarchical structure, also known as internal VM groups. Options include:
  - `-all` List all the internal VM groups
  - `-D,--detect` Detect mode lists only the internal VM groups with missing priming tag or snapshot
  - `-h,--help` Print the available usage and options for this command

  After you run the `list` command, you can see qualified internal VMs presented in a hierarchical structure known as internal VM groups. For these internal VM groups, you can run these commands:

  - `unprotect` Unprotect some or all the internal VM groups using these options:
    - `-all` Unprotect all the internal VMs. Without the `-I` option, you must specify `-all` to unprotect all the internal VM groups
    - `-I,--index` Unprotect a certain internal VM group
    - `-h,--help` Print the available usage and options for this command
  - `delete` Delete some or all the internal VM groups
  - `output` Output the internal VM groups into a disk file.
    - `-F,--file` File name to save the internal VM groups
    - `-h,--help` Print the available usage and options for this command
  - `back` Return to the main menu

- `unprotect` unprotect some or all the internal VMs, including folders. Options include:
  - `-A,--adDomain` Domain name
  - `-H,--host` Host name
  - `-D,--datastore` Datastore name
  - `-T,--vmType` Internal VM type: template, replica, or parent
  - `-N,--name` Internal VM name
  - `-I,--includeFolders` Include the internal VM folders
  - `-all` Unprotect all the internal VMs
  - `-h,--help` Print the available usage and options for this command
- `delete` delete some or all internal VMs, including folders. Options include:
  - `-A,--adDomain` Domain name
  - `-H,--host` Host name
  - `-D,--datastore` Datastore name
  - `-T,--vmType` Internal VM type: template, replica, or parent
  - `-N,--name` Internal VM name
  - `-I,--includeFolders` Include the internal VM folders
  - `-all` Delete all the internal VMs
  - `-h,--help` Print the available usage and options for this command

- `exit` Log out from vCenter Server and quit the program

Create and Manage Automated Full-Clone Desktop Pools

8

With an automated desktop pool that contains full-clone virtual machines, you create a virtual machine template and VMware Horizon 8 uses that template to create virtual machine desktops.

Depending on how you want the golden image to be managed, you can change the golden image and snapshot source in your pool from vCenter Server to Image Catalog or reverse. You must rebuild the virtual machine associated with the edited template source for the change to take effect. For more information on the Image Management Service, see the *Managing Horizon Images from the Cloud* document.

Read the following topics next:

- Worksheet for Creating an Automated Full-Clone Desktop Pool
- Create an Automated Full-Clone Desktop Pool
- Manually Customizing Machines in an Automated Desktop Pool
- Desktop Settings for Automated Full-Clone Desktop Pools
- Configuring 3D Rendering for Full-Clone Virtual Machine Pools
- Configure Full Clones with VMware vSphere Virtual Machine Encryption
- Rebuild a Virtual Machine in a Full-Clone Desktop Pool

Worksheet for Creating an Automated Full-Clone Desktop Pool

When you create an automated desktop pool of full clones, you can configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines

Category	Option	Description	Enter Your Value Here
Type	Select **Automated Desktop Pool**.		
vCenter Server	Select **Full Virtual Machines** and select the vCenter Server that manages the virtual machines in the pool.		
User assignment		The following settings determine how end users are assigned to the desktops in this pool.	
	Select **Floating** or **Dedicated**.	Choose the type of user assignment: ■ With a floating-assignment full clone, users get a random desktop every time they log in. When a user logs out, the desktop is returned to the pool and another user can log into that desktop. ■ With a dedicated-assignment full clone, each desktop is assigned to a specific user. Once a user is assigned a desktop, no other user can use the desktop. Users receive the same machine each time they log in.	
	Enable Automatic Assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user. You can assign machines manually even when automatic assignment is enabled. See Assign a Machine to a User in a Dedicated-Assignment Pool.	
	Enable Multi-User Assignment	In a dedicated-assignment pool, you can assign multiple users to each machine in the pool. Multi-user assignment is not supported for automatic user assignment desktop pools. If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users will be unable to launch a session on that machine. See Assign a Machine to a User in a Dedicated-Assignment Pool.	
Storage Optimization	Storage Policy Management: ■ **Use VMware Virtual SAN** ■ **Do not use VMware Virtual SAN**	Specify whether to use VMware vSAN, if available. vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
Desktop Pool Identification		The following settings allow you to identify and describe the pool you are creating.	
	ID	The unique name that identifies the pool in Horizon Console. If multiple vCenter Server instances are running in your environment, make sure that another vCenter Server is not using the same pool ID. You cannot edit or change the Desktop Pool ID after you create the desktop pool.	
	Display Name	The pool name that users see when they log in from a client device. If you do not specify a display name, the pool ID is displayed to users.	
	Access Group	Select an access group in which to place the pool or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. **Note** Access groups are different from vCenter Server folders that store desktop virtual machines. You select a vCenter Server folder later in the wizard with other vCenter Server settings.	
Provisioning Settings		The following settings allow you to provide details on how the pool is provisioned.	
	Enable Provisioning	You can enable or deactivate virtual machine provisioning in the desktop pool. When you deactivate provisioning in the desktop pool, VMware Horizon 8 stops provisioning new virtual machines for the desktop pool. After you deactivate provisioning, you can enable provisioning again. Before you change a desktop pool's configuration, you can deactivate provisioning to ensure that no new machines are created with the old configuration. You can also deactivate provisioning to prevent Horizon 8 from using additional storage when a pool is close to filling up the available space. When you create a desktop pool and deactivate this option, Horizon 8 creates a desktop pool without any virtual machines. If you edit a desktop pool and deactivate provisioning, Horizon 8 does not allow any new virtual machines to be provisioned in this desktop pool. End users can still connect to existing virtual machines.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Stop Provisioning on Error	You can direct Horizon 8 to stop provisioning or continue to provision virtual machines in a desktop pool after an error occurs during the provisioning of a virtual machine. If you leave this setting selected, you can prevent a provisioning error from recurring on multiple virtual machines.	
	Virtual Machine Naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines.	
	Specify Names Manually	If you specify names manually, prepare a list of machine names and, optionally, the associated user names.	
	Start machines in maintenance mode		
	# Unassigned Machines Kept Powered On	The number must be a valid integer greater than 0 and less than or equal to the maximum number of names specified. The default is 1.	
	Use a Naming Pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine.	
	Provision Machines: ■ Machines on Demand ■ All Machines Up-Front	If you use a naming pattern and provision machines on demand, specify a minimum number of machines in the pool. The minimum number of machines is created when you create the pool. If you provision machines on demand, additional machines are created as users connect to the pool for the first time or as you assign machines to users.	
	Maximum number of machines	If you use a naming pattern, specify the total number of machines in the pool. You can also specify a minimum number of machines to provision when you create the pool.	
	Number of spare (powered on) machines	If you specify names manually or use a naming pattern, specify how many machines to keep available and powered on for new users. When you specify names manually, this option is called **# Unassigned machines kept powered on**.	
	Virtual Device: Add vTPM Device to VMs	Select the check box to add a Virtual Trusted Platform Module (vTPM) device to VMs. This option does not apply to Linux VMs.	
vCenter Settings		The following settings describe vCenter Server attributes for the pool of desktops.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Virtual Machine Template	Select the virtual machine template to use for creating the pool.	
	VM Folder Location	Select the folder in vCenter Server in which the desktop pool resides.	
	Host or Cluster	Select the ESXi host or cluster on which the virtual machines run.	
	Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	
	Datastores	Choose the type of datastore: ■ **Individual datastore**. Select individual datastores on which to store the desktop pool. ■ **Storage DRS**. Select the Storage Distributed Resource Scheduler (DRS) cluster that contains shared or local datastores. Storage DRS is a load balancing utility that assigns and moves storage workloads to available datastores. **Note** If you use vSAN, there is only one datastore.	
	Network	Select the network to use for this pool or use the same network as the golden image.	
Desktop Pool Settings		The following settings determine the desktop state, power status, and display protocol when a virtual machine is not in use.	
	State	■ **Enabled**. After being created, the desktop pool is enabled and ready for immediate use. ■ **Disabled**. After being created, the pool is disabled and not available for use, and provisioning is stopped for the pool. Select this setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance. When this state is in effect, remote desktops are unavailable for use.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Connection Server Restrictions	■ **No Restrictions**. The desktop pool can be accessed by any Connection Server instance. ■ **Restrictions to these Tags**. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. If you intend to provide access to desktops through VMware Workspace ONE, and you configure Connection Server restrictions, the Workspace ONE catalog might display desktops to users when those desktops are actually restricted. Workspace ONE users will be unable to launch these desktops.	
	Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices. For more information, see "Configuring Shortcuts for Entitled Pools" in the *Horizon 8 Administration* document.	
	Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	
	Session Type	You can enable the VM Hosted Applications feature by selecting the supported session type for the desktop pool: ■ **Desktop**. Select this option to use the pool as a regular desktop pool. All the virtual machines in the pool can only be used to host desktops. ■ **Application**. Select this option to use all the virtual machines in the pool to host applications. ■ **Desktop and Application.** When this option is selected, the virtual machine in the pool can either host a regular desktop session or host an application session. The first connection to the particular virtual machine will determine the session type of the virtual machine. For more information about the VM Hosted Applications feature, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at https://techzone.vmware.com.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Remote Machine Power Policy	Determines how a virtual machine behaves when the user logs off of the associated desktop. For descriptions of the power policy options, see Power Policies for Desktop Pools. For more information about how power policies affect automated pools, see How Power Policies Affect Automated Desktop Pools.	
	Log Off After Disconnect	■ **Immediately**. Users are logged out when they disconnect. ■ **Never**. Users are never logged out. ■ **After**. The time after which users are logged off when they disconnect. Type the duration in minutes. The logout time applies to future disconnections. If a desktop session is already disconnected when you set a logout time, the logout duration for that user starts when you set the logout time, not when the session was originally disconnected. For example, if you set this value to 5 minutes, and a session was disconnected 10 minutes earlier, Horizon 8 will log out of that session 5 minutes after you set the value.	
	Bypass Session Timeout (Application and Desktop and Application session types)	Enable this setting to allow application sessions to run forever. When enabled, all the application sessions belonging to the desktop pool are never disconnected automatically, neither when reaching the max session timeout nor when reaching the global idle timeout. This setting is available when you select session types **Application** and **Desktop or Application**. Application sessions that run forever are supported on Windows and Linux clients. You cannot enable this setting if any of the applications belonging to the desktop pool is part of Global Application Entitlement as local pools. This setting is not available for application pools in a cloud pod architecture environment. Application sessions that run forever are not supported for unauthenticated users. Do not enable this setting if the max session timeout value is set to **Never**. When you restart Connection Server, existing forever running application sessions no longer run indefinitely.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Allow Users to Restart Machines	Allow users to reset or restart their own desktops.	
	Empty session timeout (Applications only)	Determines the duration of time that an empty application session remains open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select **Never**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select Immediate, the session logs off or disconnects within 30 seconds. For Windows sessions, you can further reduce the time before the session logs off or disconnects by editing a registry key on the RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session log off to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session log off to 5 seconds.	
	Pre-launch session timeout (Applications only)	Determines the timeout for the application session before the session is disconnected or logged off.	
	When timeout occurs (Applications only)	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged out frees up resources, but opening an application takes longer. The default is **Disconnect**.	
	Show Assigned Machine Name	Displays the host name of the assigned machine instead of the desktop pool display name when you log in to Horizon Client. If no machine is assigned to the user, then **Display Name (No Machine Assigned)** appears for the desktop pool when you log in to Horizon Client.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Show Machine Alias Name	Displays the machine alias name set for the assigned users of the machine instead of the desktop display name for the desktop pool in Horizon Client. Applies only to dedicated desktop entitlements. If no machine alias name is set but the **Show Assigned Machine Name** is set, then the machine host name appears for the desktop pool in Horizon Client. Otherwise, the desktop display name appears for the desktop pool in Horizon Client.	
	Delete machine on Logoff	Select whether to delete floating assignment, full-clone virtual machines. ■ **No**. Virtual machines remain in the desktop pool after users log out. ■ **Yes**. Virtual machines are powered off and deleted as soon as users log out. This option is not applicable for dedicated assignment, full clone virtual machines.	
Remote Display Settings		The following settings describe how desktops are displayed to end users.	
	Default Display Protocol	For a Windows pool, the choices are VMware Blast, PCoIP, and Microsoft RDP. For a Linux pool, VMware Blast is the only display protocol supported. The protocols are described as follows. ■ **VMware Blast**. The VMware Blast Extreme protocol is built on the H.264 protocol and supports the broadest range of client devices, including smart phones, tablets, ultra-low-cost PCs, and Macs, across any network. ■ **PCoIP**. PCoIP is supported as the display protocol for virtual and physical machines that have Teradici hardware. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN. ■ **Microsoft RDP**. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.	
	Allow Users to Choose Protocol	Allow users to override the default display protocol for their desktops in Horizon Client. This option is not applicable to Linux pools.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	3D Renderer	You can configure the 3D Renderer to use software rendering or hardware rendering based on physical GPU graphics cards installed on hosts. If you select RDP as the Default Display Protocol, you must enable the **Allow users to choose protocol** setting (select **Yes**) to enable 3D rendering. If the default display protocol is RDP and you disable the **Allow users to choose protocol** setting (select **No**), the 3D rendering option is disabled. With the hardware-based 3D Renderer options, users can take advantage of graphics applications for design, modeling, and multimedia. With the software 3D Renderer option, users can take advantage of graphics enhancements in less demanding applications such as AERO, Microsoft Office, and Google Earth. For more details, see Configuring 3D Rendering for Full-Clone Virtual Machine Pools. When you edit this setting, you must power off existing virtual machines, verify that the machines are reconfigured in vCenter Server, and power on the machines to cause the new setting to take effect. Restarting a virtual machine does not cause the new setting to take effect.	
	VRAM Size	The amount of 3D VRAM allocated to each desktop.	
	Maximum Number of Monitors	If you select PCoIP or VMware Blast as the display protocol, you can select the maximum number of monitors on which users can display the desktop. You can select up to four monitors. When the 3D Renderer setting is not selected, the Max number of monitors setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the number of monitors, more memory is consumed on the associated ESXi hosts. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Maximum Resolution of Any One Monitor	If you select PCoIP or VMware Blast as the display protocol, you should specify the maximum resolution of any one monitor. The maximum resolution of any one monitor is set to 1920 x 1200 pixels by default, but you can configure this value. When the 3D Renderer setting is not selected, the Max resolution of any one monitor setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the resolution, more memory is consumed on the associated ESXi hosts. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.	
	Allow Session Collaboration	Select **Enabled** to allow users of the desktop pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast protocol.	
Advanced Storage Options		The following settings are for advanced storage options.	
	Use View Storage Accelerator	Determine whether ESXi hosts cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is enabled by default. **Note** The Horizon console does not save the blackout times if you add or delete blackout times and then disable View Storage Accelerator.	
	Regenerate Storage Accelerator After	Select the number of days to regenerate the Storage Accelerator. Add blackout days and times in the **Set Blackout Days** window.	

Table 8-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (continued)

Category	Option	Description	Enter Your Value Here
	Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you activate TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by VMware Horizon 8 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	
Guest Customization	Guest customization	For a Windows pool, select a customization specification (SYSPREP) from the list to configure licensing, domain attachment, DHCP settings, and other properties on the machines. You can only select a customization specification that matches the guest operating system of the template. For a Linux pool, ClonePrep is the only customization method supported. Alternatively, you can customize the machines manually after they are created.	
	Allow Reuse of Existing Computer Accounts	Select this option to allow reuse of previously used machine names. **Note** Rebuild operation does not take this setting into consideration and always reuses the machine name.	

Create an Automated Full-Clone Desktop Pool

You can create an automated full-clone desktop pool based on a Windows or Linux virtual machine (VM) template that you select. VMware Horizon 8 dynamically deploys the desktops, creating a new virtual machine in vCenter Server for each desktop.

Prerequisites

- Prepare a virtual machine template that Horizon 8 will use to create the machines. Horizon Agent must be installed on the template. See Chapter 3 Creating and Preparing a Virtual Machine for Cloning.

  You create virtual machine templates in vSphere Client. You can create a virtual machine template from a previously configured virtual machine, or you can convert a previously configured virtual machine to a virtual machine template.

  For information on using vSphere Client to create virtual machine templates, see the *vSphere Virtual Machine Administration* guide on the VMware vSphere Documentation portal.
- For a Windows machine, if you intend to use a customization specification, make sure that the specifications are accurate. In vSphere Client, deploy and customize a virtual machine from your template using the customization specification. Fully test the resulting virtual machine, including DHCP and authentication.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESXi host must equal or exceed the number of virtual machines multiplied by the number of virtual NICs per virtual machine.
- Verify that vCenter Server is added to Horizon Connection Server.
- Verify that you have prepared the virtual machine for cloning. See .Chapter 3 Creating and Preparing a Virtual Machine for Cloning.
- The following requirements apply to Linux machines:
  - If you use the Winbind solution to join the Linux virtual machine to Active Directory, you must finish configuring the Winbind solution in the virtual machine template.
  - If you use the Winbind solution, you must run the domain join command on the virtual machine. Include the command in a shell script and specify the script path to the Horizon Agent option `RunOnceScript` in `/etc/vmware/viewagent-custom.conf`. For more information, see Edit Configuration Files on a Linux Desktop.
  - Create a guest customization specification.

    See "Create a Customization Specification for Linux" in *vSphere Virtual Machine Administration* on the VMware vSphere Documentation portal. Fully test the capabilities of the virtual machine created using the specification, including DHCP and authentication.

    When you create the specification, make sure that you specify the following settings correctly.

Setting	Value
Target Virtual Machine OS	Linux
Computer Name	Use the virtual machine name.

Setting	Value
Domain	Specify the domain of the Horizon 8 environment.
Network Settings	Use standard network settings.
Primary DNS	Specify a valid address.

Note To create a guest customization specification for a Debian machine in vSphere 7.0, follow the steps described in VMware Knowledge Base (KB) article 85845. For more information on the Guest OS Customization Support Matrix, see http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf.

- Gather the configuration information you must provide to create the pool. See Worksheet for Creating an Automated Full-Clone Desktop Pool.
- If you intend to provide access to your desktops and applications through VMware Workspace ONE Access, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in Horizon Console. If you give the user the Administrators role on an access group other than the root access group, VMware Workspace ONE Access will not recognize the SAML authenticator you configure in Horizon 8, and you cannot configure the pool in VMware Workspace ONE Access.

Procedure

1. In Horizon Console, select **Inventory > Desktops**.
2. Click **Add**.
3. Select **Automated Desktop Pool** and click **Next**.
4. Select **Full Virtual Machines**, select the vCenter Server instance, and click **Next**.
5. Follow the prompts to create the pool.

   Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page by clicking the page name in the navigation pane.

What to do next

Entitle users to access the pool. See "Entitling Users and Groups" in *Horizon 8 Administration* on the VMware Horizon Documentation portal.

Manually Customizing Machines in an Automated Desktop Pool

After you create an automated pool, you can customize particular machines without reassigning ownership. By starting the machines in maintenance mode, you can modify and test the machines before you release them to users.

Maintenance mode prevents users from accessing their desktops. If you start machines in maintenance mode, VMware Horizon 8 places each machine in maintenance mode when the machine is created. In a dedicated-assignment pool of full virtual machines, you can use maintenance mode to log in to a machine without having to reassign ownership to your own administrator account. When you finish the customization, you do not have to return ownership to the user assigned to the machine.

To perform the same customization on all machines in an automated pool, customize the virtual machine you prepare as a template. Horizon 8 deploys your customization to all the machines.

Note You can start machines in maintenance mode if you manually specify machine names for the pool, not if you name machines by providing a naming pattern.

Customize Machines by Placing Them in Maintenance Mode After Pool Creation

After an automated desktop pool is created, you can customize, modify, or test individual machines by placing them in maintenance mode. When a machine is in maintenance mode, users cannot access the virtual machine desktop.

You place existing machines in maintenance mode one at a time. You can remove multiple machines from maintenance mode in one operation.

When you create a desktop pool, you can start all the machines in the pool in maintenance mode if you specify machine names manually.

Procedure

1. In Horizon Console, select **Inventory > Desktops**.
2. Click the link for the pool.
3. Select the **Machines** tab.
4. Select a machine.
5. Select **Enter Maintenance Mode** from the **More Commands** drop-down menu.
6. Customize, modify, or test the virtual machine desktop.
7. Repeat steps to select a machine and customize, modify, or test the virtual machine desktop.
8. Select the customized machines and select **Exit Maintenance Mode** from the **More Commands** drop-down menu.

Results

The modified virtual machine desktops are available to users.

Customize Machines by Starting Them in Maintenance Mode During Pool Creation

You can customize individual machines after an automated pool is created by starting the machines in maintenance mode.

Procedure

1 In Horizon Console, begin creating an automated desktop pool by starting the **Add Pool** wizard.

2 On the Provisioning Settings page, select **Specify names manually**.

3 Select **Start machines in maintenance mode**.

4 Complete the **Add Pool** wizard to finish creating the desktop pool.

5 In vCenter Server, log in, customize, and test the individual virtual machines.

   You can customize Windows machines manually or by using standard Windows systems-management software such as Altiris, SMS, LanDesk, or BMC.

6 In Horizon Console, select **Inventory > Machines**.

7 Select specific machines to release to your users.

8 Click **More Commands > Exit Maintenance Mode**.

What to do next

Notify your users that they can log in to their desktops.

Desktop Settings for Automated Full-Clone Desktop Pools

You must specify desktop pool settings when you configure automated pools that contain full-clone virtual machines. Different settings apply to pools with dedicated user assignments and floating user assignments.

Settings for Automated Pools That Contain Full-Clone Virtual Machines lists the differences in settings.

Table 8-2. Settings for Automated Pools That Contain Full-Clone Virtual Machines

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
State	Yes	Yes
Connection Server restrictions	Yes	Yes
Remote machine power policy	Yes	Yes
Automatic logoff after disconnect	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes

Table 8-2. Settings for Automated Pools That Contain Full-Clone Virtual Machines (continued)

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
Allow user to initiate separate sessions from different client devices		Yes
Delete machine after logoff		Yes
Default display protocol	Yes	Yes
Allow users to choose protocol	Yes	Yes
3D Renderer	Yes	Yes
Max number of monitors	Yes	Yes
Max resolution of any one monitor	Yes	Yes
Override global Mirage settings	Yes	Yes
Mirage Server configuration	Yes	Yes
Enable Multi-User Assignment	Yes	
Display Assigned Machine Name	Yes	

Configuring 3D Rendering for Full-Clone Virtual Machine Pools

When you create or edit a desktop pool of virtual machines, you can configure 3D graphics rendering for your desktops.

End users can take advantage of 3D applications for design, modeling, and multimedia, which typically require GPU hardware to perform well. For users that do not require physical GPU, a software option provides graphics enhancements that can support less demanding applications such as Windows AERO, Microsoft Office, and Google Earth. Following are brief descriptions of the 3D graphics options:

NVIDIA GRID vGPU (shared GPU hardware acceleration)

This feature allows a physical GPU on an ESXi host to be shared among virtual machines and offers flexible hardware-accelerated 3D profiles ranging from lightweight 3D task workers to high-end workstation graphics power users. NVIDIA GRID vGPU is the only 3D graphics option supported for Linux desktops.

AMD MxGPU - for Windows desktops only

This feature allows multiple virtual machines to share an AMD GPU by making the GPU appear as multiple PCI passthrough devices and offers flexible hardware-accelerated 3D profiles, ranging from lightweight 3D task workers to high-end workstation graphics power users.

Virtual Dedicated Graphics Acceleration (vDGA) - for Windows desktops only

This feature dedicates a single physical GPU on an ESXi host to a single virtual machine. Use this feature if you require high-end, hardware-accelerated workstation graphics.

Note See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

Virtual Shared Graphics Acceleration (vSGA) - for Windows desktops only

This feature allows multiple virtual machines to share the physical GPUs on ESXi hosts and is suitable for mid-range 3D design, modeling, and multimedia applications.

Soft 3D - for Windows desktops only

Software-accelerated graphics allow you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical GPU. Use this feature for less demanding 3D applications such as Windows Aero themes, Microsoft Office 2010, and Google Earth.

AMD MxGPU and vDGA solutions do not support VMotion. NVIDIA GRID vGPU, vSGA and Soft 3D support VMotion.

In some cases, if an application such as a video game or 3D benchmark forces the desktop to display in full screen resolution, the desktop session can be disconnected. Possible workarounds include setting the application to run in Windowed mode or matching the VMware Horizon 8 session desktop resolution to the default resolution expected by the application.

3D Renderer Options for Full-Clone Virtual Machine Pools

The **3D Renderer** setting for full-clone virtual machine pools provides options that let you configure graphics rendering in different ways.

The following table describes the differences between the various types of 3D rendering options available in VMware Horizon 8, but does not provide complete information for configuring virtual machines and ESXi hosts for Virtual Shared Graphics Acceleration (vSGA), Virtual Dedicated Graphics Acceleration (vDGA), AMD MxGPU, and NVIDIA GRID vGPU. These tasks must be done with vSphere Client before you attempt to create desktop pools in Horizon Console. For details on these tasks, see NVIDIA vGPU Deployment Guide for VMware Horizon and Preparing for AMD MxGPU for Windows Full-Clone VMs.

Table 8-3. 3D Renderer Options

Option	Description
Manage using vSphere Client	The **3D Renderer** option that is set in vSphere Web Client for a virtual machine determines the type of 3D graphics rendering that takes place. Horizon 8 does not control 3D rendering. In the vSphere Client, you can configure the **Automatic**, **Software**, or **Hardware** options. These options have the same effect as they do when you set them in Horizon Console. Use this setting when configuring vDGA and AMD MxGPU. This setting is also an option for vSGA. This setting is not applicable to Linux desktops. When you select the **Manage using vSphere Client** option, the **Configure VRAM for 3D Guests**, **Max number of monitors**, and **Max resolution of any one monitor** settings are inactive in Horizon Console. You can configure the amount of memory in vSphere Client.
Automatic	3D rendering is enabled. The ESXi host controls the type of 3D rendering that takes place. For example, the ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. If all GPU hardware resources are already reserved when a virtual machine is powered on, ESXi uses the software renderer for that machine. This setting is an option when configuring vSGA. This setting is not applicable to Linux desktops. The ESXi host allocates VRAM to a virtual machine based on the value that is set in the **Configure VRAM for 3D Guests** dialog box.
Software	3D rendering is enabled. The ESXi host uses software 3D graphics rendering. If a GPU graphics card is installed on the ESXi host, this pool will not use it. Use this setting to configure Soft 3D. This setting is not applicable to Linux desktops. The ESXi host allocates VRAM to a virtual machine based on the value that is set in the **Configure VRAM for 3D Guests** dialog box.
Hardware	3D rendering is enabled. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. This setting is an option when configuring vSGA. This setting is not applicable to Linux desktops. The ESXi host allocates VRAM to a virtual machine based on the value that is set in the **Configure VRAM for 3D Guests** dialog box. **Important** If you configure the **Hardware** option, consider these potential constraints: ■ If a user tries to connect to a machine when all GPU hardware resources are reserved, the virtual machine will not power on, and the user will receive an error message. ■ If you use vMotion to move the machine to an ESXi host that does not have GPU hardware configured, the virtual machine will not power on. When you configure hardware-based 3D rendering, you can examine the GPU resources that are allocated to each virtual machine on an ESXi host. For details, see Examining GPU Resources on an ESXi Host.

Table 8-3. 3D Renderer Options (continued)

Option	Description
NVIDIA GRID vGPU	3D rendering is enabled for NVIDIA GRID vGPU. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. If a user tries to connect to a machine when all GPU hardware resources are being used by other virtual machines on the host, Connection Server will attempt to move the virtual machine to another ESXi host in the cluster before powering on. Use this setting when configuring NVIDIA GRID vGPU. When you select the **NVIDIA GRID vGPU** option, the **Configure VRAM for 3D Guests**, **Max number of monitors**, and **Max resolution of any one monitor** settings are inactive in Horizon Console. When you configure the golden image virtual machine or virtual machine template with vSphere Web Client, you are prompted to reserve all memory. **Important** If you configure the **NVIDIA GRID vGPU** option, consider these potential constraints: ■ The virtual machine cannot be suspended or resumed. Therefore the Remote Machine Power Policy option for suspending the virtual machine is not available. ■ If you use vMotion to move the machine to an ESXi host that does not have GPU hardware configured, the virtual machine will not power on. Live vMotion is not available. ■ All ESXi hosts in the cluster must be version 6.0 or later, and the virtual machines must be hardware version 11 or later. ■ If an ESXi cluster contains a host that is NVIDIA GRID vGPU enabled and a host that is not NVIDIA GRID vGPU enabled, the hosts display a yellow (warning) status in the Horizon Console Dashboard. If a user tries to connect to a machine when all GPU hardware resources are being used by other virtual machines on the host, Connection Server will attempt to move the virtual machine to another ESXi host in the cluster before powering on. In this case, hosts that are not NVIDIA GRID vGPU enabled cannot be used for this type of dynamic migration.
Disabled	3D rendering is inactive.

Best Practices for Configuring 3D Rendering For Full-Clone Virtual Machine Pools

The 3D rendering options and other pool settings offer various advantages and drawbacks. Select the option that best supports your vSphere hardware infrastructure and your users' requirements for graphics rendering.

Note For detailed information about all the various choices and requirements for 3D rendering, see the VMware white paper about graphics acceleration. Since Linux desktops only support NVIDIA GRID vGPU for 3D rendering, some of the choices described on this page are not applicable to Linux desktops.

When to Choose the Automatic Option for Windows Desktops

The **Automatic** option is the best choice for many Horizon 8 deployments that require 3D rendering. vSGA (Virtual Shared Graphics Acceleration)-enabled virtual machines can dynamically switch between software and hardware 3D rendering, without your having to reconfigure. This option ensures that some type of 3D rendering takes place even when GPU resources are completely reserved.

The only drawback with the **Automatic** option is that you cannot easily tell whether a virtual machine is using hardware or software 3D rendering.

When to Choose the Hardware Option for Windows Desktops

The **Hardware** option guarantees that every virtual machine in the pool uses hardware 3D rendering, provided that GPU resources are available on the ESXi hosts. This option might be the best choice when all your users run graphically intensive applications. You can use this option when configuring vSGA (Virtual Shared Graphics Acceleration).

With the **Hardware** option, you must strictly control your vSphere environment. All ESXi hosts must have GPU graphics cards installed.

When all GPU resources on an ESXi host are reserved, Horizon 8 cannot power on a virtual machine for the next user who tries to log in to a desktop. You must manage the allocation of GPU resources and the use of vMotion to ensure that resources are available for your desktops.

When to Choose the Option to Manage Windows Machines Using vSphere Client

When you select the **Manage using vSphere Client** option, you can use vSphere Client to configure individual virtual machines with different options and VRAM values.

- For vSGA (Virtual Shared Graphics Acceleration), you can support a mixed configuration of 3D rendering and VRAM sizes for virtual machines in a pool.
- For vDGA (Virtual Dedicated Graphics Acceleration), each virtual machine must be individually configured to share a specific PCI device with the ESXi host and all memory must be reserved. For more information, see Preparing for vDGA Capabilities for Windows Full-Clone VMs.

  All ESXi hosts must have GPU graphics cards installed.

  Note See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

- For AMD MxGPU, each virtual machine must be individually configured to share a specific PCI device with the ESXi host and all memory must be reserved. This feature allows a PCI device to appear to be multiple separate physical PCI devices so that the GPU can be shared between 2 to 15 users. For more information, see Preparing for AMD MxGPU for Windows Full-Clone VMs.

  All ESXi hosts must be version 6.0 or later and must have GPU graphics cards installed.

You might also choose this option if you want to explicitly manage graphics settings of clones by having the clones inherit settings from the golden image virtual machine.

When to Choose the NVIDIA GRID vGPU Option

With the **NVIDIA GRID vGPU** option, you can achieve a higher consolidation ratio of virtual machines on an NVIDIA GRID vGPU-enabled ESXi host than is possible by using vDGA, while maintaining the same performance level. As with vDGA (Dedicated Virtual Graphics), the ESXi and virtual machine also use GPU pass-through for NVIDIA GRID vGPU.

Note To improve virtual machine consolidation ratios, you can set the ESXi host to use consolidation mode. Edit the `/etc/vmware/config` file on the ESXi host and add the following entry:

```
vGPU.consolidation = "true"
```

By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is called performance mode. If you would rather have the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU, you can use consolidation mode.

Because a GPU does not need to be dedicated to one specific virtual machine, with the **NVIDIA GRID vGPU** option, you can create and configure a golden image virtual machine or virtual machine template to be NVIDIA GRID vGPU-enabled and then create a desktop pool of virtual machines that can share the same physical GPU.

If all GPU resources on an ESXi host are being used by other virtual machines, when the next user tries to log in to a desktop, Horizon 8 can move the virtual machine to another NVIDIA GRID vGPU-enabled ESXi server in the cluster and then power on the virtual machine. All ESXi hosts must be version 6.0 or later and must have GPU graphics cards installed.

For more information, see Preparing for NVIDIA GRID vGPU Capabilities for Full-Clone VMs.

When to Choose the Software Option for Windows Desktops

Select the **Software** option if your ESXi hosts do not have GPU graphics cards, or if your users only run applications such as AERO and Microsoft Office, which do not require hardware graphics acceleration.

Configuring Desktop Settings to Manage GPU Resources

You can configure other desktop settings to ensure that GPU resources are not wasted when users are not actively using them.

For floating pools, set a session timeout so that GPU resources are freed up for other users when a user is not using the desktop.

For dedicated pools, you can configure the **Automatically logoff after disconnect** setting to **Immediately** and a **Suspend** power policy if these settings are appropriate for your users. For example, do not use these settings for a pool of researchers who execute long-running simulations. Note that the **Suspend** power policy is not available if you use the **NVIDIA GRID vGPU** option.

Preparing for NVIDIA GRID vGPU Capabilities for Full-Clone VMs

NVIDIA GRID vGPU provides direct access to the physical GPU on an ESXi host, allowing multiple virtual machines (VMs) to share a single GPU using vendor graphics card drivers.

Follow these instructions to configure VMs and ESXi hosts to create NVIDIA GRID vGPU-enabled desktop pools in VMware Horizon 8. For complete information and detailed procedures, see the NVIDIA vGPU Deployment Guide for VMware Horizon.

1. Verify the host machine is supported in the VMware Compatibility Guide, and check with the vendor to verify the host meets power and configuration requirements. Install the graphics card in the ESXi host.
2. Verify that the guest virtual machines run with virtual hardware version 11 or later. Configure the virtual machine template to use a shared PCI device before you create the desktop pool in Horizon 8. For detailed instructions, see the NVIDIA vGPU Deployment Guide for VMware Horizon.
3. Download the NVIDIA vSphere Installation Bundle (VIB) for the appropriate version of ESXi. VIBs are compatible with major version releases. For instance, the NVIDIA ESXi 6.5 VIB works with ESXi 6.5U2, but will not work with ESXi 6.7.
4. Update VMware Tools and Virtual Hardware (vSphere Compatibility) for the template or each VM that will use vGPU.
5. In vSphere Client, edit the VM settings and add a shared PCI device. PCI devices require reserving guest memory. Expand **New PCI Device** and click **Reserve all guest memory**. You can also modify this setting in the VM Memory settings.
6. Select the appropriate GPU Profile for your use case. For sizing guidelines, see NVIDIA vGPU Deployment Guide for VMware Horizon.
7. Download the NVIDIA Guest Driver installer package to the VM. Make sure it matches the version of the installed NVIDIA VIB on ESXi.
8. Choose one of the following methods to install the NVIDIA Guest Driver. After the NVIDIA driver is installed, vCenter Server console will display a black screen.

   - Desktop Pool
   - View Agent Direct-Connection Plug-in
   - RDP - for Windows machines only

   See the sections later on this page for more details about each installation method.

vMotion of vGPU Virtual Machines

- vMotion of vGPU Virtual Machines is supported starting with vSphere 6.7. See here for details on how to configure this and more information.
- vSphere Distributed Resource Scheduler (DRS) in vSphere 6.7 Update 1 and later supports initial placement of vGPU VMs without load balancing support.

- DRS in vSphere 6.7 or vSphere 7.0 versions earlier than vSphere 7.0 U3f will not automatically vMotion vGPU VMs when ESXi hosts are placed in maintenance mode. An administrator is required to manually initiate vMotion of vGPU VMs in order to allow ESXi hosts to enter maintenance mode.
- DRS in vSphere 7.0 U3f and later can be configured to allow automatic vMotion when hosts are placed in maintenance mode. See https://kb.vmware.com/s/article/88271 for instructions. DRS load balancing remains unsupported for vGPU VMs.

Desktop Pool

This method is for creating a template VM.

1 Install Horizon Agent.
2 Configure domain and other network settings, as needed.
3 Configure the VMs as desktops in the pool.
4 Assign admin level access to accounts.
5 Connect Horizon Client to Horizon Console to access desktops.
6 Install NVIDIA driver, reboot, and reconnect.
7 Access NVIDIA Control Panel and enter license server information.

Horizon Agent Direct-Connection Plug-in

This method is for a quick environment verification, or a simple user level access.

1 Install Horizon Agent.
2 Install the matching Horizon Agent Direct-Connection Plug-in. You need local administrator account access.
3 Log in with Horizon Client. Use the VM IP address as Connection Server.
4 Install NVIDIA driver, reboot, and reconnect.
5 Access NVIDIA Control Panel and enter license server information.

RDP

This method is for creating a template VM before installing Horizon Agent.

1 Enable Remote Desktop access in the VMs.
2 Log in using Microsoft Remote Desktop Connection.
3 Install NVIDIA driver, reboot, and reconnect.
4 Access NVIDIA Control Panel and enter license server information.
5 Install Horizon Agent.
6 Configure domain and other network settings, as needed.

In the **Add Desktop Pool** wizard, select the NVIDIA GRID vGPU option for 3D Renderer and only NVIDIA GRID vGPU-enabled ESXi hosts and NVIDIA GRID vGPU-enabled virtual machine templates appear for selection in the wizard. VMware recommends using the default Blast settings for the pool protocol. For additional protocol options and other advanced configuration settings, consult the *NVIDIA GRID vGPU User Guide*.

You can use the same vGPU profile for a mix of full clones and instant clones. If you use different vGPU profiles for a mix of full clones and instant clones, avoid creating or powering on full clones and instant clones at the same time.

If you are using multiple vGPU profiles, set the host assignment policy of all GPU hosts within a cluster to **GPU consolidation**. For a single vGPU profile that is used by all the desktops, set assignment policy of all GPU hosts within a cluster to **Best Performance**.

Preparing for vDGA Capabilities for Windows Full-Clone VMs

Virtual Dedicated Graphics Acceleration (vDGA) provides direct pass-through to a physical GPU, providing a user with unrestricted, dedicated access to a single GPU. Before you attempt to create a Windows desktop pool that has vDGA capabilities, you must perform certain configuration tasks on the virtual machines (VMs) and ESXi hosts.

vDGA is supported for Windows desktops only. This overview is an outline of tasks you must perform in vSphere before you can create or configure desktop pools in Horizon Console.

Note See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

1. Install the graphics card on the ESXi host.
2. Verify that VT-d or AMD IOMMU is enabled on the ESXi host.
3. Enable pass-through for the GPU in the ESXi host configuration and reboot.
4. Add a PCI device to the virtual machine and select the appropriate PCI device to enable GPU pass-through on the virtual machine.
5. Reserve all memory when creating the virtual machine.
6. Configure virtual machine video card 3D capabilities.
7. Obtain the GPU drivers from the GPU vendor and install the GPU device drivers in the guest operating system of the virtual machine.
8. Install VMware Tools and Horizon Agent in the guest operating system and reboot.
9. The virtual machines must be virtual hardware version 9 or later.

10 Enable GPU pass-through on the ESXi hosts and configure the individual virtual machines to use dedicated PCI devices after the desktop pool is created in Horizon 8. You cannot configure the golden image virtual machine or template for vDGA and then create a desktop pool, because the same physical GPU would be dedicated to every virtual machine in the pool.

11 Set the 3D Renderer option to **Manage using vSphere Client**.

After you perform these tasks, you must add the virtual machine to a manual desktop pool so that you can access the guest operating system using PCoIP or VMware Blast Extreme. In a PCoIP or VMware Blast session, you can then activate the NVIDIA, AMD, or Intel display adapter in the guest operating system.

Preparing for AMD MxGPU for Windows Full-Clone VMs

With AMD MxGPU, multiple Windows virtual machines (VMs) share an AMD GPU by making the GPU appear as multiple PCI passthrough devices. AMD MxGPU provides direct pass-through to a physical GPU, providing a user with unrestricted, dedicated access to a single GPU.

AMD MxGPU is supported for Windows desktops only. Before you attempt to create a desktop pool that has capabilities to use AMD MxGPU, you must perform certain configuration tasks on the virtual machines and ESXi hosts.

This overview is an outline of tasks you must perform in vSphere before you can create or configure desktop pools in Horizon 8.

1 Install the graphics card on the ESXi host.

2 Install the GPU vSphere Installation Bundle (VIB).

3 Verify that SR-IOV and VT-d or AMD IOMMU are enabled on the ESXi host.

4 Use the `esxcfg-module` command to configure the graphics card for SR-IOV (Single Root I/O Virtualization) .

   See Configuring AMD MxGPU for Windows Full-Clone Machines.

5 Reboot the ESXi host.

6 Add a PCI device to the virtual machine and select the appropriate PCI device to enable GPU pass-through on the virtual machine.

7 Verify that the guest virtual machines have virtual hardware version 11 or later.

8 Reserve all memory when creating the virtual machine.

9 Configure virtual machine video card 3D capabilities.

10 Obtain the GPU drivers from the GPU vendor and install the GPU device drivers in the guest operating system of the virtual machine.

11 Install VMware Tools and Horizon Agent in the guest operating system and reboot.

12 Set the 3D Renderer option to **Manage using vSphere Client**.

After you perform these tasks, you must add the virtual machine to a manual desktop pool so that you can access the guest operating system using PCoIP or VMware Blast Extreme. If you attempt to access the virtual machine using a vSphere, the display will show a black screen.

Configuring AMD MxGPU for Windows Full-Clone Machines

You use the `esxcfg-module` command-line command to configure such parameters as the number of users who can share the GPU, the amount of frame buffer allocated to each user, and some performance control.

Syntax

```
esxcfg-module -s "adapter1_conf=bus#,device#,function#,number_of_VFs,FB_size,time_slice,mode"
amdgpuv
```

Usage Notes

The `vicfg-module` command supports setting and retrieving VMkernel module options on an ESXi host. For general reference information about this command, see the *vSphere Command-Line Interface Reference* documentation at https://code.vmware.com.

Required Flags

You must specify several flags when configuring AMD MxGPU. If the command does not include all the required flags, no error message is provided, but the configuration defaults to a simple 4 SR-IOV device configuration.

Table 8-4. Flags for Configuring AMD SR-IOV

Flag	Description
bus#	Bus number in decimal format.

device#	PCIe device ID for the supported AMD card, in decimal format. To see a list, use the command `lspci | grep -i display`.
	For example, for a system that has two AMD GPU cards, you might see the following output when you run this command:
	`[root@host:~] lspci | grep -i display`
	`0000:04:00.0 Display controller:`
	`0000:82:00.0 Display controller:`
	In this example, the PCIe device IDs are 04 and 82. Note that these IDs are listed in hexadecimal format and must be converted to decimal format for use in the `vicfg-module` command .
	AMD S7150 cards support only a single GPU per card, and so the device ID and function ID are 0 for these cards.

function#	Function number in decimal format.
number_of_VFs	Number of VFs (virtual functions), from 2 to 15. This number represents the number users who will share the GPU.

Table 8-4. Flags for Configuring AMD SR-IOV (continued)

Flag	Description
FB_size	Amount of fame buffer memory, in MB, allocated to each VF. To determine the size, take the overall amount of video memory on the card and divide that amount by the number of VFs. Then round that number to the nearest number that is a multiple of 8. For example, for an AMD S7150 card, which has 8000 MB, you could use the following settings; ■ For 2 VFs, use 4096. ■ For 4 VFs, use 2048. ■ For 8 VFs, use 1024. ■ For 15 VFs, use 544.
time_slice	Interval between VF switches, in microseconds. This setting adjusts the delay in queuing and processing commands between the SR-IOV devices. Use a value between 3000 and 40000. Adjust this value if you see significant stuttering when multiple SR-IOV desktops are active.
mode	Following are the valid values: 0 = reclaimed performance; 1 = fixed percentage performance.

Important After you run the `esxcfg-module` command, you must reboot the ESXi host for the settings to take effect.

Examples

1 For a single AMD S7150 card on PCI ID 4 shared between 8 users:

```
esxcfg-module -s "adapter1_conf=4,0,0,8,1024,4000" amdgpuv
```

2 For a single server with two AMD S7150 cards on PCI ID 4 and PCI ID 82 shared between 4 power users:

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,2,4096,4000"
amdgpuv
```

3 For a single server with two AMD S7150 cards, you can set each card with different parameters. For instance if your View environment needs to support 2 power users and 16 task workers:

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,15,544,7000"
amdgpuv
```

4 Enable the SR-IOV option on the ESXi host.

Some hosts have SR-IOV as a configurable option in the BIOS.

Preparing to Use vSGA for Windows Full-Clone VMs

vSGA allows multiple Windows virtual machines (VMs) to share the physical GPUs on ESXi hosts.

To support vSGA, a pool must meet these additional requirements:

- GPU graphics cards and the associated vSphere Installation Bundles (VIBs) must be installed on the ESXi hosts. For a list of supported GPU hardware, see the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php.
- The virtual machines must be virtual hardware version 10 or later, and be running Wndows.
- You can set the 3D Renderer option to any of the following settings: **Manage using vSphere Client**, **Automatic**, or **Hardware**. See Video RAM Configuration Options for the 3D Renderer. **Automatic** uses hardware acceleration if there is a capable and available hardware GPU in the ESXi host. If a hardware GPU is not available, the virtual machine uses software 3D rendering for any 3D tasks.

Preparing to Use Soft 3D for Windows Full-Clone VMs

When you enable Soft 3D, the ESXi host uses software 3D graphics rendering.

To support software 3D rendering, a pool must meet these additional requirements:

- The virtual machines (VMs) must be virtual hardware version 8 or later, and be running Windows.
- You must set the 3D Renderer option to **Software**. See Video RAM Configuration Options for the 3D Renderer.

Video RAM Configuration Options for the 3D Renderer

With video RAM configuration, you can configure the amount of VRAM that is assigned to the virtual machines in the pool. The information on this page applies to Windows pools only.

When you enable the 3D Renderer setting and select the **Automatic**, **Software**, or **Hardware** option, you can configure the amount of VRAM that is assigned to the virtual machines in the pool by moving the slider in the **Configure VRAM for 3D guests** box. The maximum VRAM size is 512MB. The default VRAM size is 96MB.

The VRAM settings that you configure in Horizon Console take precedence over the VRAM settings that can be configured for the virtual machines in vSphere Client or the vSphere Web Client, unless you select the **Manage using vSphere Client** option.

Configure Full Clones with VMware vSphere Virtual Machine Encryption

You can configure full clones to use the vSphere Virtual Machine Encryption feature. You can create full-clone desktops that have the same encryption keys or full-clone desktops with different keys.

Prerequisites

- Create the Key Management Server (KMS) cluster with key management servers.

- To create a trust between KMS and vCenter Server, accept the self-signed certificate or create a certificate signed by a Certificate Authority (CA).
- In vSphere Client, create the `VMcrypt/VMEncryption` storage profile.

Note For details about the Virtual Machine Encryption feature in vSphere, see the *vSphere Security* document in the VMware vSphere Documentation portal.

Procedure

1 To configure full clones that use the same encryption keys, create a virtual machine (VM) template for all desktops to have the same encryption keys.

   The clone inherits the parent encryption state including keys.

   a In vSphere Client, create a VM with the `vmencrypt` storage policy.

   b Convert the VM to a virtual machine template.

   c Create full-clone desktops that point to the template VM so that all desktops have the same encryption keys.

   Note VM Encryption and Content Based Read Cache (CBRC) are not compatible. To use VM Encryption, you must turn off CBRC globally by turning off View Storage Accelerator in Horizon Console by navigating to **Settings > Servers**.

2 To configure full clones that use different encryption keys, you must change the storage policy for each full-clone desktop.

   a In vSphere Client, create the full-clone desktop pool and then edit the full-clone desktops.

      You can also edit existing full-clone desktops.

   b Navigate to each full-clone desktop and edit the storage policy and change the storage policy to `vmencrypt`.

      Each full-clone desktop gets a different encryption key.

Rebuild a Virtual Machine in a Full-Clone Desktop Pool

Rebuild a virtual machine in a full-clone desktop pool if you want to replace the virtual machine with a new virtual machine and want to reuse the machine name. For example, you can rebuild a virtual machine that is in an error state to replace the virtual machine with an error free virtual machine of the same name.

When you rebuild a virtual machine, the virtual machine is deleted and then cloned with the same virtual machine name and the AD computer accounts are reused. All user data or settings from the previous virtual machine are lost and the new virtual machine is created using the desktop pool template.

Prerequisites

- Create an automated full-clone desktop pool. See Create an Automated Full-Clone Desktop Pool.

Procedure

1. In Horizon Console, select **Inventory > Desktops**.
2. Select the desktop pool that contains the virtual machine you want to rebuild and click the **Inventory** tab.
3. Select the virtual machine that you want to rebuild and click **Rebuild**.

   In vCenter Client, you can view the virtual machine as it is deleted and cloned again with the same name. In Horizon Console, the status of the rebuilt virtual machine goes through the following states: **Deleting > Provisioning > Customizing > Available**.

Creating and Managing Manual Desktop Pools

9

Use a manual desktop pool if you have pre-existing groups of desktops that you want to manage with VMware Horizon 8. You can create manual desktop pools for both single-session desktops and multi-session desktops.

Compared to an automated desktop pool, a manual desktop pool has limited features. For example, Horizon 8 does not manage the lifecycle of the desktops in a manual desktop pool. Instant clones are not applicable to manual desktop pools.

Horizon 8 supports the following types of manual desktop pools.

Manual Desktop Pool of VMware vSphere Machines

This type of manual desktop pool contains the following types of virtual machine:

- Independent virtual machines that are managed by vCenter Server.

These vSphere virtual machines are not created by Horizon 8. For example, these machines were created in vSphere by another virtual desktop infrastructure software and now you want to migrate them to Horizon 8.

To create a manual desktop pool of vSphere virtual machines, you must install Horizon Agent on each machine, and then select the **vCenter virtual machines** option as part of the manual desktop pool creation workflow.

Instant-clone technology is not supported on this type of manual desktop pool. This type of manual desktop pool is also different from automated full-clone desktop pools in which Horizon 8 creates a pool of virtual machines that are cloned from a template VM as part of the pool creation process.

Manual Desktop Pool of Non-vSphere Machines

This type of manual desktop pool contains the following types of machines:

- Non-vSphere virtual machines. Virtual machines that run on a virtualization platform other than vCenter Server.
- Physical machines.

When these machines get registered with Connection Server as part of the Horizon Agent installation process, these machines are called registered machines. To create a manual desktop pool that contains non-vSphere VMs or physical machines in Horizon Console, you must select the **Other sources** option as part of the manual desktop pool creation workflow.

After you create this type of manual desktop pool, you can view these non-vSphere virtual machines or physical computers in Horizon Console by navigating to **Settings > Registered Machines > Others**.

RDS hosts are also registered machines that are not managed by vSphere. For more information on RDS hosts, see Introduction to Multi-session Published Desktops and Applications.

Note After the virtual machine is added to a manual pool in Horizon 8, you need to power off the machine so the new display settings can be applied. These settings include monitor count, monitor resolution, and the Screen DMA setting. For more information, see https://kb.vmware.com/s/article/2144475.

Read the following topics next:

- Manual Pool of VMware vSphere Virtual Machines
- Manual Pool of Registered Non-vSphere Virtual Machines
- Manual Pool of Registered Physical Machines
- Prepare a non-vSphere Machine For VMware Horizon 8 Management
- Worksheet for Creating a Manual Desktop Pool
- Desktop Pool Settings for Manual Pools in Horizon Console
- Running Windows Virtual Machines on Hyper-V
- Create a Manual Desktop Pool
- Managing non-vSphere Registered Machines

Manual Pool of VMware vSphere Virtual Machines

Complete the following steps in the workflow to create a manual desktop pool that contains vSphere virtual machines.

- Prepare the machines to deliver remote desktop access. In a manual pool that contains vSphere virtual machines, you must prepare each machine individually. Horizon Agent must be installed and running on each machine. To prepare vSphere virtual machines managed by vCenter Server, see Chapter 3 Creating and Preparing a Virtual Machine for Cloning.
- Gather the configuration information that you must provide to create the pool. See Worksheet for Creating a Manual Desktop Pool .
  - Power policies are supported for manual desktop pools that contain vSphere virtual machines. See Setting Power Policies for Desktop Pools.

  - 3D rendering options are supported for manual desktop pools that contain vSphere virtual machines. These options are also supported for full-clone desktop pools. For more information, see Configuring 3D Rendering for Full-Clone Virtual Machine Pools.
- Create the manual desktop pool and select the **vCenter virtual machines** option to select the vSphere virtual machine as the desktop pool source. See Create a Manual Desktop Pool.
- Entitle users to access the manual desktop pool. See "Entitling Users and Groups" in the *Horizon 8 Administration* document.

Manual Pool of Registered Non-vSphere Virtual Machines

Non-vSphere virtual machines run on a virtualization platform other than vCenter Server. Since these machines get registered with Connection Server as part of the Horizon Agent installation process, these machines are called registered non-vSphere virtual machines. To create a manual desktop pool that contains non-vSphere virtual machines in Horizon Console, you must select the **Other sources** option as part of the manual desktop pool creation workflow.

Complete the following steps in the workflow to create a manual desktop pool that contains registered non-vSphere virtual machines.

- Prepare the non-vSphere virtual machine to deliver remote desktop access. Before you add this virtual machine to a manual desktop pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine. To prepare non-vSphere virtual machines, see Prepare a non-vSphere Machine For VMware Horizon 8 Management.
- Gather the configuration information that you must provide to create the pool. See Worksheet for Creating a Manual Desktop Pool .
  - Power policies are not supported for manual desktop pools that contain registered non-vSphere virtual machines because these machines are not directly managed by vSphere.
  - 3D rendering options are not applicable for manual desktop pools that contain registered non-vSphere virtual machines. However, these virtual machines can directly leverage GPU capability available to the Horizon Agent operating system. Verify the graphics support with the third-party virtualization platform vendor.
- Create the manual desktop pool and select the **Other sources** option to select the registered non-vSphere virtual machine as the desktop pool source. See Create a Manual Desktop Pool.
- Entitle users to access the manual desktop pool. See "Entitling Users and Groups" in the *Horizon 8 Administration* document.
- Perform management tasks on non-vSphere registered machines. See Managing non-vSphere Registered Machines.

Manual Pool of Registered Physical Machines

A registered physical machine is a physical computer that has Horizon Agent installed and is then registered with Connection Server.

Creating a manual desktop pool that contains registered physical machines provides end users access to their corporate physical computers remotely in a convenient and secure manner. Teleworkers who need access to their physical machines that reside within the corporate office can also access their machines without requiring to be on VPN and compromising security.

Both floating and dedicated user assignments are supported. With dedicated assignments, you can also manually assign individual desktops so that each employee is connected to their own physical machine. You can also create a manual desktop pool with a single registered physical machine to enable single user access for the physical machine in the desktop pool.

With dedicated assignments, you can also assign multiple users to each physical machine in a desktop pool so that shift workers can share the same desktop instead of reserving the dedicated machine for each user.

Physical machines support NVIDIA GPUs and encoders. Physical machines can also directly leverage GPU capability available to the Horizon Agent operating system. When physical Windows workstations (Desktop or Server OS) have Horizon Agent loaded on them directly, the OpenGL acceleration of the GPU might be limited in some cases:

- For Intel and AMD GPUs, the Direct3D and OpenGL capabilities of the card can be used in remote sessions.
- For NVIDIA GeForce GPUs, the Direct3D capabilities is used in the remote session. For OpenGL, see the downloadable tool at https://developer.nvidia.com/designworks or https://developer.nvidia.com/nvidia-opengl-rdp
- For systems with more than one GPU, for example, an integrated Intel for general workloads and a discrete AMD or NVIDIA for 3D workloads, deactivate the integrated card so the 3D graphics card is used.

The following NVIDIA series have been tested:

- NVIDIA Studio Driver 546.01
- NVIDIA Ampere series
- NVIDIA Titan series
- GeForce RTX 40 series
- GeForce RTX 30 series
- GeForce RTX 20 series
- GeForce GTX 16 series
- GeForce GTX 10 series
- Quadro Series
- M4000
- P4000
- K620

The following Intel series have been tested:

- Intel Graphics DCH Driver 101.5122
- Intel Gen10 series
- Intel Gen11 series
- Intel Gen12 series

Complete the following steps in the workflow to create a manual desktop pool that contains registered physical machines.

- Prepare the physical machine to deliver remote desktop access. Before you add this physical machine to a manual desktop pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine. To prepare non-vSphere virtual machines, see Prepare a non-vSphere Machine For VMware Horizon 8 Management.
- Gather the configuration information that you must provide to create the pool. See Worksheet for Creating a Manual Desktop Pool . The following options are not supported for manual desktop pools that contain registered physical machines:
  - Power policies are not supported.
  - PCoIP is not supported.
- Create the manual desktop pool and select the **Other sources** option to select the registered non-vSphere virtual machine as the desktop pool source. See Create a Manual Desktop Pool.
- Entitle users to access the manual desktop pool. See "Entitling Users and Groups" in the *Horizon 8 Administration* document.
- Perform management tasks on non-vSphere registered machines. See Managing non-vSphere Registered Machines.

Note Manual desktop pools that contain registered physical machines supports Wake-on-LAN. This feature enables the entitled user to wake up the physical machine while connecting from Connection Server. Wake-on-LAN is supported with the VMware Blast protocol for dedicated-assignment manual desktop pools that contain registered physical machines. For more information about Wake-on-LAN, see "VMware Blast Extreme" in the *Horizon Overview and Deployment Planning* document.

For more information about using physical machines, see the "Using Horizon 7 to Access Physical Windows Machines" document available at https://techzone.vmware.com.

Prepare a non-vSphere Machine For VMware Horizon 8 Management

You must perform certain tasks to prepare a non-vSphere machine to be managed by Horizon 8.

Prerequisites

- Verify that you have administrative rights on the non-vSphere machine.
- To make sure that remote desktop users are added to the local Remote Desktop Users group of the non-vSphere machine, create a restricted Remote Desktop Users group in Active Directory. See the *Horizon 8 Installation and Upgrade* document for more information.

Procedure

1. Power on the non-vSphere machine and verify that it is accessible to the Connection Server instance.
2. Join the non-vSphere machine to the Active Directory domain for your remote desktops.
3. Configure the Windows firewall to allow Remote Desktop connections to the non-vSphere machine.

What to do next

Install Horizon Agent on the non-vSphere machine. See Install Horizon Agent on a Non-vSphere Machine.

Install Horizon Agent on a Non-vSphere Machine

You must install Horizon Agent on an all non-vSphere machines. VMware Horizon cannot manage a non-vSphere machine unless Horizon Agent is installed.

To install Horizon Agent on multiple Windows physical computers without having to respond to wizard prompts, you can install Horizon Agent silently.

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon 8 Installation and Upgrade* document.
- Verify that you have administrative rights on the non-vSphere machine.
- To use a non-vSphere Windows Server machine as a remote desktop rather than as an RDS host, perform the steps described in Prepare Windows Server Operating Systems for Desktop Use.
- Familiarize yourself with the Horizon Agent custom setup options for non-vSphere machines.
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *Horizon Overview and Deployment Planning* document for more information.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.

Procedure

1 To start the Horizon Agent installation program, double-click the installer file.

The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

2 Accept the VMware license terms.

3 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

You must install all VMware Horizon components with the same IP version.

4 Select whether to enable or disable FIPS mode.

This option is available only if FIPS mode is enabled in Windows.

5 Select your custom setup options.

6 Accept or change the destination folder.

7 In the **Server** text box, type the host name or IP address of a Connection Server host.

During installation, the installer registers the non-vSphere machine with this Connection Server instance. After registration, the specified Connection Server instance, and any additional instances in the same Connection Server group, can communicate with the non-vSphere machine.

8 Select an authentication method to register the non-vSphere machine with the Connection Server instance.

Option	Action
Authenticate as the currently logged in user	The **Username** and **Password** text boxes are disabled and you are logged in to the Connection Server instance with your current username and password.
Specify administrator credentials	You must provide the username and password of a Connection Server administrator in the **Username** and **Password** text boxes.

Provide the username in the following format: **`Domain\User`**.

The user account must be a domain user with access to Horizon Directory on the Connection Server instance. A local user does not work.

9 Follow the prompts in the Horizon Agent installation program and finish the installation.

10 If you selected the USB redirection option, restart the non-vSphere machine to enable USB support.

In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the non-vSphere machine.

Results

The Horizon Agent service is started on the non-vSphere machine and the machine is registered with Horizon 8.

What to do next

Use the registered non-vSphere machine to create a manual desktop pool. See Create a Manual Desktop Pool.

After the pool is created, you can edit the pool.

Note When you reconfigure a pool setting that affects a registered machine, it can take up to 10 minutes for the new setting to take effect. For example, if you change the **Automatically logoff after disconnect** setting for a pool, Horizon 8 might take up to 10 minutes to reconfigure the affected machines.

Horizon Agent Custom Setup Options for Non-vSphere Machines

When you install Horizon Agent on a non-vSphere machine, you can select or deselect certain custom setup options. In addition, Horizon Agent installs certain features automatically on all guest operating systems on which they are supported. These features are not optional.

To change custom setup options after you install the latest Horizon Agent version, you must uninstall and reinstall Horizon Agent. For patches and upgrades, you can run the new Horizon Agent installer and select a new set of options without uninstalling the previous version.

Table 9-1. Horizon Agent Features That Are Installed Automatically on Non-vSphere Machines in an IPv4 Environment (Not Optional)

Feature	Description
PCoIP Agent	Lets users connect to the remote desktop with the PCoIP display protocol. The PCoIP Agent feature is supported on physical machines that are configured with a Teradici TERA host card.
Lync	Provides support for Microsoft Lync 2013 Client on remote desktops.
Unity Touch	Allows tablet and smart phone users to interact easily with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications, all without using the Start menu or Taskbar.

Table 9-2. Horizon Agent Custom Setup Options for Non-vSphere Machines in an IPv4 Environment (Optional)

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops. USB redirection is supported on remote desktops that are deployed on single-user machines. In addition, redirection of USB flash drives and hard disks is supported on RDS desktops and applications. This setup option is not selected by default. You must select the option to install it. For guidance on using USB redirection securely, see the *Horizon Security* document. For example, you can use group policy settings to disable USB redirection for specific users.
Client Drive Redirection	Allows Horizon Client users to share local drives with their remote desktops. After this setup option is installed, no further configuration is required on the remote desktop. Client Drive Redirection is also supported on VDI desktops that run on managed, single-user virtual machines and on RDS desktops and applications.
Smartcard Redirection	Lets users authenticate with smart cards when they use the PCoIP or Blast Extreme display protocol. Smartcard Redirection is supported on remote desktops that are deployed on single-user machines but is not supported on RDS host-based remote desktops.
Virtual audio driver	Provides a virtual audio driver on the remote desktop.

In an IPv6 environment, the only optional feature is Smartcard Redirection.

In an IPv6 environment, the only automatically installed feature is PCoIP Agent.

Worksheet for Creating a Manual Desktop Pool

When you create a manual desktop pool, you can configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

Note In a manual pool, you must prepare each machine to deliver remote desktop access. Horizon Agent must be installed and running on each machine before you can add the machine to the manual desktop pool.

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool

Option	Description	Enter Your Value Here
vCenter Server	The vCenter Server that manages the machines. This option appears only if the machines are virtual machines that are managed by vCenter Server.	
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a machine. After a user is assigned a desktop, no other user can use the desktop. Users receive the same machine each time they log in. ■ In a floating-assignment pool, users receive different machines each time they log in. For details, see Assign a Machine to a User in a Dedicated-Assignment Pool.	
Enable automatic assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user. You can assign machines manually even when automatic assignment is enabled.	
Enable Multi-User Assignment	In a dedicated-assignment pool, you can assign multiple users to each machine in the pool. Multi-user assignment is not supported for automatic user assignment desktop pools. If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users will be unable to launch a session on that machine.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Machine Source	The virtual machines or physical computers that you want to include in the desktop pool. 1 Decide which type of machine you want to use. You can use virtual machines that are managed by vCenter Server, virtual machines that are managed by another virtualization platform, or physical computers. 2 Prepare a list of the machines that you want to include in the desktop pool. 3 Install Horizon Agent on each machine that you want to include in the desktop pool. To use PCoIP with machines that are unmanaged virtual machines or physical computers, you must use Teradici hardware. Only Windows machines support PCoIP. **Note** When you enable Windows Server desktops in Horizon Console, the console displays all available Windows Server machines, including machines on which Connection Server and other Horizon 8 software are installed, as potential machine sources. You cannot select machines for the desktop pool if Horizon 8 software is installed on the machines. Horizon Agent cannot coexist on the same virtual or physical machine with any other Horizon 8 software component, including Connection Server or Horizon Client.	
Desktop Pool ID	The pool name that users see when they log in and that identifies the pool in Horizon Console. If multiple vCenter Server instances are running in your environment, make sure that another vCenter Server is not using the same pool ID. A Connection Server configuration can be a standalone Connection Server instance or a pod of replicated instances that share a common LDAP configuration.	
Display name	The pool name that users see when they log in from a client. If you do not specify a name, the pool ID is used.	
Access group	Select an access group for the pool or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. **Note** Access groups are different from vCenter Server folders that store desktop VMs.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
State	- **Enabled**. After being created, the desktop pool is enabled and ready for immediate use. - **Disabled**. After being created, the desktop pool is deactivated and unavailable for use. This is an appropriate setting if you want to conduct activities such as testing or other forms of baseline maintenance. When this state is in effect, remote desktops are unavailable for use.	
Connection Server restrictions	- **None**. The desktop pool can be accessed by any Connection Server instance. - **With tags**. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. If you intend to provide access to your desktops through VMware Workspace ONE Access, and you configure Connection Server restrictions, the Workspace ONE catalog might display desktops to users when those desktops are actually restricted. Workspace ONE users will be unable to launch these desktops.	
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices. For more information, see "Configuring Shortcuts for Entitled Pools" in the *Horizon 8 Administration* document.	
Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Session Types	You can enable the VM Hosted Applications feature by selecting the supported session type for the desktop pool: ■ **Desktop**. Select this option to use the pool as a regular desktop pool. All the virtual machines in the pool can only be used to host desktops. ■ **Application**. Select this option to use all the virtual machines in the pool to host applications. ■ **Desktop and Application.** When this option is selected, the virtual machine in the pool can either host a regular desktop session or host an application session. The first connection to the particular virtual machine will determine the session type of the virtual machine. For more information about the VM Hosted Applications feature, see the technical marketing white paper "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" available at https://techzone.vmware.com.	
Remote machine power policy	Determines how a virtual machine behaves when the user logs out from the associated desktop. This option is only available for a manual pool of vSphere virtual machines. For descriptions of the power policy options, see Power Policies for Desktop Pools.	
Logoff after disconnect	■ **Immediately**. Users are logged out as soon as they disconnect. ■ **Never**. Users are never logged out. ■ **After**. The time after which users are logged out when they disconnect. Type the duration in minutes. The logout time applies to future disconnections. If a desktop session was already disconnected when you set a logout time, the logout duration for that user starts when you set the logout time, not when the session was originally disconnected. For example, if you set this value to five minutes, and a session was disconnected 10 minutes earlier, Horizon 8 will log out that session five minutes after you set the value.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Empty session timeout (Applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select **Never**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select **Immediate**, the session logs you out or disconnects within 30 seconds. You can further reduce the time the session logs out or disconnects by editing a registry key on a Windows RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.	
Pre-launch session timeout (Applications only)	Determines the timeout for the application session before the session is disconnected or logged out.	
When timeout occurs	Determines whether an empty application session is disconnected or logged out after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged out frees up resources, but opening an application takes longer. The default is **Disconnect**.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Bypass Session Timeout (Application and Desktop and Application session types)	Enable this setting to allow application sessions to run forever. When enabled, all the application sessions belonging to the desktop pool will never be disconnected automatically, neither when reaching the max session timeout nor when reaching the global idle timeout. This setting is available when you select session types **Application** and **Desktop or Application**. Application sessions that run forever are supported on Windows and Linux clients. You cannot enable this setting if any of the applications belonging to the desktop pool is part of Global Application Entitlement as local pools. This setting is not available for application pools in a cloud pod architecture environment. Application sessions that run forever are not supported for unauthenticated users. Do not enable this setting if the max session timeout value is set to **Never**. When you restart Connection Server, existing forever running application sessions no longer run indefinitely.	
Allow users to reset/restart their machines	Allow users to reset or restart their own desktops.	
Show Assigned Machine Name	Displays the host name of the assigned machine instead of the desktop pool display name when you log in to Horizon Client. If no machine is assigned to the user then, **Display Name (No Machine Assigned)** appears for the desktop pool when you log in to Horizon Client.	
Show Machine Alias Name	Displays the machine alias name set for the assigned users of the machine instead of the desktop display name for the desktop pool in Horizon Client. Applies only to dedicated desktop entitlements. If no machine alias name is set but the **Show Assigned Machine Name** is set, then the machine host name appears for the desktop pool in Horizon Client. Otherwise, the desktop display name appears for the desktop pool in Horizon Client.	
Allow Machine Name Selection	Enabling this option will allow a command line launch of Horizon Client to specify a machine name to connect to, for example for test or troubleshooting purposes. Applies only to floating desktop pools.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Default Display Protocol	**VMware Blast**. The VMware Blast Extreme protocol is built on the H.264 protocol and supports the broadest range of client devices, including smart phones, tablets, ultra-low-cost PCs, and Macs, across any network. **PCoIP**. PCoIP is supported as the display protocol for virtual and physical Windows machines that have Teradici hardware. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN. **Microsoft RDP**. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a Windows computer remotely.	
Allow Users to Choose Protocol	Allow users to override the default display protocol for their desktops in Horizon Client. This option is not applicable to Linux pools.	
3D Renderer	You can configure the 3D Renderer to use software rendering or hardware rendering based on physical GPU graphics cards installed on hosts. If you select RDP as the Default Display Protocol, you must enable the **Allow users to choose protocol** setting (select **Yes**) to enable 3D rendering. If the default display protocol is RDP and you disable the **Allow users to choose protocol** setting (select **No**), the 3D rendering option is disabled. With the hardware-based 3D Renderer options, users can take advantage of graphics applications for design, modeling, and multimedia. With the software 3D Renderer option, users can take advantage of graphics enhancements in less demanding applications such as AERO, Microsoft Office, and Google Earth. For more details, see Configuring 3D Rendering for Full-Clone Virtual Machine Pools. For a Linux pool, use vSphere Client for 2D desktops and NVIDIA GRID vGPU for 3D desktops. When you edit this setting, you must power off existing virtual machines, verify that the machines are reconfigured in vCenter Server, and power on the machines to cause the new setting to take effect. Restarting a virtual machine does not cause the new setting to take effect.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Max Number of Monitors	If you select PCoIP or VMware Blast as the display protocol, you can select the maximum number of monitors on which users can display the desktop. You can select up to four monitors. When the 3DRenderer setting is not selected, the Max number of monitors setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the number of monitors, more memory is consumed on the associated ESXi hosts. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.	
Max Resolution of Any One Monitor	If you select PCoIP or VMware Blast as the display protocol, you should specify the maximum resolution of any one monitor. The maximum resolution of any one monitor is set to 1920 x 1200 pixels by default, but you can configure this value. When the 3D Renderer setting is not selected, the Max resolution of any one monitor setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the resolution, more memory is consumed on the associated ESXi hosts. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. When you edit the pool, you must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
HTML Access	Select **Enabled** to allow users to connect to remote desktops from within their Web browsers. When a user logs in through the VMware Horizon Web portal page or the Workspace ONE app and selects a remote desktop, the HTML Access agent enables the user to connect to the desktop over HTTPS. The desktop is displayed in the user's browser. Other display protocols, such as PCoIP or RDP, are not used. Horizon Client software does not have to be installed on the client devices. To use HTML Access, you must install HTML Access in your VMware Horizon 8 deployment. For more information, see the *Horizon HTML Access Guide* on the VMware Horizon Documentation portal. To use HTML Access with VMware Workspace ONE Access, you must pair Connection Server with a SAML Authentication server, as described in the *Horizon 8 Administration* document. VMware Workspace ONE Access must be installed and configured for use with Connection Server.	
Allow Session Collaboration	Select **Enabled** to allow users of the pool to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast display protocol.	
Allow user to initiate separate sessions from different client devices	Allow user to initiate separate sessions from different client devices	

Table 9-3. Worksheet: Configuration Options for Creating a Manual Desktop Pool (continued)

Option	Description	Enter Your Value Here
Use View Storage Accelerator	Determine whether ESXi hosts cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is enabled by default. **Note** Horizon Console does not save the restriction times if you add or delete restriction times and then deactivate View Storage Accelerator. The View Storage Accelerator feature takes effect for new virtual machines of a newly created manual pool only after the new virtual machines are powered off once and powered on.	
Transparent Page Sharing Scope	This option is only available for a manual pool of vSphere virtual machines. Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you activate TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by VMware Horizon 8 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	

Desktop Pool Settings for Manual Pools in Horizon Console

The desktop pool settings you can configure when you create a manual desktop pool differs depending on the type of machines and user assignments.

Registered machines include registered non-vSphere virtual machines and registered physical machines.

Table 9-4. Settings for Manual Desktop Pools

Setting	vSphere virtual machines, Dedicated Assignment	vSphere virtual machines, Floating Assignment	Registered Machines, Dedicated Assignment	Registered Machines, Floating Assignment
State	Yes	Yes	Yes	Yes
Connection Server restrictions	Yes	Yes	Yes	Yes
Remote machine power policy	Yes	Yes		
Automatically logoff after disconnect	Yes	Yes	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes		
Allow user to initiate separate sessions from different client devices		Yes		Yes
Default display protocol	Yes	Yes	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.
Allow users to choose protocol	Yes	Yes	Yes	Yes
3D Renderer	Yes	Yes		
Max number of monitors	Yes	Yes		
Max resolution of any one monitor	Yes	Yes		
Enable automatic user assignment	Yes		Yes	

Table 9-4. Settings for Manual Desktop Pools (continued)

Setting	vSphere virtual machines, Dedicated Assignment	vSphere virtual machines, Floating Assignment	Registered Machines, Dedicated Assignment	Registered Machines, Floating Assignment
Enable Multi-User Assignment	Yes		Yes	
Display Assigned Machine Name	Yes		Yes	

Running Windows Virtual Machines on Hyper-V

VMware Horizon supports virtual machines running on Hyper-V hypervisor version Hyper-V Server 2016 and Hyper-V Server 2019.

The following operating systems are supported:

- VDI: Windows 10 21H2 64-bit, Windows 10 22H2 64-bit, Windows 11 21H2 64-bit, Windows 11 22H2 64-bit
- RDS Hosts: Windows Server 2016 Standard 64-bit, Windows Server 2019 (Hyper-V Server 2016, Hyper-V Server 2019), and Windows Server 2022 (Hyper-V Server 2019)

Running Horizon Agent in virtual machines on Hyper-V has the following limitations and known issues:

- Horizon Agent installation in Desktop mode is not supported on Windows Server OS.
- When you click the CAD button on the Hyper-V console, the CAD window also displays on the remote desktop session.
- Hyper-V does not support GPU-related features: vGPU, 3D RDSH, HEVC.

  Note Hyper-V based virtual machines can directly leverage GPU capability available to the Horizon Agent operating system. Verify the graphics support with the third-party virtualization platform vendor (Microsoft).

Create a Manual Desktop Pool

You can create a manual desktop pool that provisions desktops from VMware vSphere virtual machines or registered machines that include non-vSphere virtual machines and physical computers.

Prerequisites

- Prepare the machines to deliver remote desktop access. In a manual pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine.

To prepare vSphere virtual machines managed by vCenter Server, see Chapter 3 Creating and Preparing a Virtual Machine for Cloning.

To prepare non-vSphere virtual machines or physical computers, see Managing non-vSphere Registered Machines.

- Gather the configuration information that you must provide to create the pool. See Worksheet for Creating a Manual Desktop Pool .

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click **Add**.

Note Do not include Windows and Linux virtual machines in the same desktop pool. If a pool contains both Windows and Linux machines, the pool is treated as a Windows pool, and users cannot connect to the Linux desktops.

3 Select **Manual Desktop Pool**.

4 Choose virtual machines managed by vCenter Server or other virtual machines that are not managed by vCenter Server and click **Next**.

Option	Description
vCenter virtual machines	vSphere virtual machines that are managed by vCenter Server. Select the vCenter Server on which the virtual machines reside.
Other Sources	Physical computers or virtual machines that are not managed by vCenter Server.

5 Follow the prompts in the wizard to create the pool.

Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

When you select the vSphere virtual machines for inclusion into the manual desktop pool, Horizon 8 ensures that a spare machine is powered on so that users can connect to it. The spare machine is powered on regardless of which power policy is in effect for the desktop pool.

Results

In Horizon Console, you can view the machines as they are added to the pool by selecting **Inventory > Desktops**.

What to do next

Entitle users to access the pool. See "Entitling Users and Groups" in the *Horizon 8 Administration* document.

Managing non-vSphere Registered Machines

In Horizon Console, you can manage non-vSphere registered machines from VMware Horizon 8.

Remove a Registered Machine from a Manual Desktop Pool

You can reduce the size of a desktop pool by removing registered machines from the pool.

Procedure

1. In Horizon Console, select **Inventory > Machines**.
2. Select the **Others** tab.
3. Select the unmanaged machines to remove.
4. Click **Remove**.
5. Click **OK**.

Results

The unmanaged machines are removed from the pool.

Remove Registered Machines From VMware Horizon 8

If you do not plan to use a registered machine again, you can remove it from Horizon 8.

After you remove a registered machine, it becomes unavailable in Horizon 8. To make the machine available again, you must reinstall Horizon Agent.

Prerequisites

Verify that the registered machines that you want to remove are not being used in any desktop pool.

Procedure

1. In Horizon Console, select **Settings > Registered Machines**.
2. Click the **RDS Hosts** tab.
3. Select one or more machines and click **Remove**.

   You can select only machines that are not being used by a desktop pool.
4. Click **OK** to confirm.

Salvaged Linked Clones

10

This page describes the background and functionality of salvaged linked clones. With salvaged linked clones, you can upgrade to VMware Horizon 8 and continue to use persistent linked clones that you created in your VMware Horizon 7 environment.

Introduction to Salvaged Linked Clones

Linked clones and View Composer were previously available in Horizon 7. They were subsequently deprecated in Horizon 8, with their functionality replaced by instant clones.

To perform an in-place upgrade from Horizon 7 to Horizon 8, you must first remove View Composer. Any linked-clone desktop pools from your Horizon 7 environment are automatically visible in Horizon 8 as salvaged linked clones.

Since View Composer is no longer supported in Horizon 8, you cannot refresh and recompose these salvaged linked clones.

Benefits of Salvaged Linked Clones

Salvaged linked clones can help you with a Horizon 8 upgrade if you have persistent linked clones in your Horizon 7 environment and are not ready to decommission them yet. Persistent linked clones are those linked clones that were never refreshed and recomposed and therefore have end-user data stored on them. In this respect, persistent linked clones resemble full clones.

By leveraging salvaged linked clones, you can migrate to Horizon 8 and continue to use your persistent linked-clone pools. This transition period gives you time to plan your move away from linked clones to instant clones or full clones. You can also consider alternatives such as VMware Dynamic Environment Manager with folder redirection for your data persistence needs.

To learn more about managing salvaged linked clones, see VMware Knowledge Base (KB) article 95767.

Configuring All Virtual Desktop Pool Types

11

When you create a virtual desktop pool, you select configuration options that determine how the pool is managed and how users interact with the desktops.

These tasks apply to virtual desktop pools that are deployed on single-user machines including full clones, instant clones, and manual desktop pools, unless otherwise noted.

If you have connected your pod to Horizon Cloud and want information on configuring virtual desktop pools for use in a Universal Broker environment, see the *Administration of Your Horizon Cloud Tenant Environment and Pod Fleet* document.

Read the following topics next:

Using a Naming Pattern for Desktop Pools

You can provision the machines in a pool by providing a naming pattern and the total number of machines you want in the pool. By default, VMware Horizon 8 uses your pattern as a prefix in all the machine names and appends a unique number to identify each machine.

Length of the Naming Pattern in a Machine Name

Machine names have a 15-character limit, including your naming pattern and the automatically generated number.

Table 11-1. Maximum Length of the Naming Pattern in a Machine Name

If You Set This Number of Machines in the Pool	This Is the Maximum Prefix Length
1-99	13 characters
100-999	12 characters
1,000 or more	11 characters

Names that contain fixed-length tokens have different length limits.

Using a Token in a Machine Name

You can place the automatically generated number anywhere else in the name by using a token. When you type the pool name, type **n** surrounded by curly brackets to designate the token.

For example: **amber-{n}-desktop**

When a machine is created, Horizon 8 replaces **{n}** with a unique number.

You can generate a fixed-length token by typing **{n:fixed=*number of digits*}**.

Horizon 8 replaces the token with numbers containing the specified number of digits.

For example, if you type **amber-{n:fixed=3}**, Horizon 8 replaces **{n:fixed=3}** with a three-digit number and creates these machine names: **amber-001**, **amber-002**, **amber-003**, and so on.

Length of the Naming Pattern When You Use a Fixed-Length Token

Names that contain fixed-length tokens have a 15-character limit, including your naming pattern and the number of digits in the token.

Table 11-2. Maximum Length of the Naming Pattern When You Use a Fixed-Length Token

Fixed-Length Token	Maximum Length of the Naming Pattern
{n:fixed=1}	14 characters
{n:fixed=2}	13 characters
{n:fixed=3}	12 characters

Machine-Naming Example

This example shows how to create two automated desktop pools that use the same machine names, but different sets of numbers. The strategies that are used in this example achieve a specific user objective and show the flexibility of the machine-naming methods.

The objective is to create two pools with the same naming convention such as VDIABC-*XX*, where *XX* represents a number. Each pool has a different set of sequential numbers. For example, the first pool might contain machines VDIABC-01 through VDIABC-10. The second pool contains machines VDIABC-11 through VDIABC-20.

You can use either machine-naming method to satisfy this objective.

- To create fixed sets of machines at one time, specify machine names manually.
- To create machines dynamically when users log in for the first time, provide a naming pattern and use a token to designate the sequential numbers.

Specifying the Names Manually

1 Prepare a text file for the first pool that contains a list of machine names from VDIABC-01 through VDIABC-10.

2 In Horizon Console, create the pool and specify machine names manually.

3 Click **Enter Names** and copy your list into the **Enter Machine Names** list box.

4 Repeat these steps for the second pool, using the names VDIABC-11 through VDIABC-20.

For detailed instructions, see Specify a List of Machine Names.

You can add machines to each pool after it is created. For example, you can add machines VDIABC-21 through VDIABC-30 to the first pool, and VDIABC-31 through VDIABC-40 to the second pool. See Add Machines to an Automated Pool Provisioned by a List of Names.

Providing a Naming Pattern With a Token

1 In Horizon Console, create the first pool and use a naming pattern to provision the machine names.

2 In the naming-pattern text box, type **`VDIABC-0{n}`**.

3 Limit the pool's maximum size to 9.

4 Repeat these steps for the second pool, but in the naming-pattern text box, type **`VDIABC-1{n}`**.

The first pool contains machines VDIABC-01 through VDIABC-09. The second pool contains machines VDIABC-11 through VDIABC-19.

Alternatively, you can configure the pools to contain up to 99 machines each by using a fixed-length token of 2 digits:

- For the first pool, type **`VDIABC-0{n:fixed=2}`**.

- For the second pool, type **`VDIABC-1{n:fixed=2}`**.

Limit each pool's maximum size to 99. This configuration produces machines that contain a 3-digit sequential naming pattern.

First pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Second pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

For details about naming patterns and tokens, see Using a Naming Pattern for Desktop Pools.

Change the Size of a Desktop Pool Provisioned by a Naming Pattern

When you provision an automated desktop pool by using a naming pattern, you can increase or decrease the size of the pool by changing the maximum number of machines.

Prerequisites

- Verify that you provisioned the desktop pool by using a naming pattern.
- Verify that the desktop pool is automated.

Procedure

1. In Horizon Console, select **Inventory > Desktops**.
2. Click the desktop pool ID and click **Edit**.
3. On the **Provisioning Settings** tab, type the new number of machines in the desktop pool in the **Max number of machines** text box.

Results

If you increase the desktop pool size, new machines can be added to the pool up to the maximum number.

If you decrease the size of a floating-assignment pool, unused machines are deleted. If more users are logged into the pool than the new maximum, the pool size decreases after users log off.

If you decrease the size of a dedicated-assignment pool, unassigned machines are deleted. If more users are assigned to machines than the new maximum, the pool size decreases after you unassign users.

Note When you decrease the size of a desktop pool, the actual number of machines might be larger than **Max number of machines** if more users are currently logged in or assigned to machines than the value that is specified in **Max number of machines**.

Naming Machines Manually or Providing a Naming Pattern in Horizon Console

With an automated desktop pool of full virtual machines or instant clones, you can specify a list of names for the desktop machines or provide a naming pattern.

If you name machines manually, each line must contain a unique machine name.

If you provide a naming pattern, VMware Horizon 8 can dynamically create and assign machines as users need them.

The following table compares the two naming methods, showing how each method affects the way you create and administer a desktop pool.

Table 11-3. Naming Machines Manually or Providing a Machine-Naming Pattern

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Machine names	The machine names are generated by appending a number to the naming pattern. For details, see Using a Naming Pattern for Desktop Pools.	Enter names that will be used to create new virtual machines. The name can be used for both floating and dedicated-assignment pools. Optionally, for dedicated desktop pools, a user name can be specified. Specific user names will be ignored for floating desktop pools. In a dedicated-assignment pool, you can pair users with machines by listing user names with the machine names. **Start machines in maintenance mode** is not applicable for dedicated and floating instant clone pools. For details, see Specify a List of Machine Names.
Pool size	You specify a maximum number of machines.	**Maximum Machines** is not available for dedicated and floating instant clone pools when virtual machines are specified manually. Your list of machine names determines the number of machines.

Table 11-3. Naming Machines Manually or Providing a Machine-Naming Pattern (continued)

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
To add machines to the pool	You can increase the maximum pool size.	You can add machine names to the list. For details, see Add Machines to an Automated Pool Provisioned by a List of Names.
On-demand provisioning	Available. Horizon 8 dynamically creates and provisions the specified minimum and spare number of machines as users first log in or as you assign machines to users. Horizon 8 can also create and provision all the machines when you create the pool.	Not available. Provisioning machines on demand is deactivated for virtual machines whose names are specified manually in both dedicated and floating pools.
Initial customization	Available. When a machine is provisioned, Horizon 8 can run a customization specification that you select.	Available. When a machine is provisioned, Horizon 8 can run a customization specification that you select.
Manual customization of dedicated machines	To customize machines and return desktop access to your users, you must remove and reassign the ownership of each machine. Depending on whether you assign machines on first log in, you might have to perform these steps twice. You cannot start machines in maintenance mode. After the pool is created, you can manually put the machines into maintenance mode.	You can customize and test machines without having to reassign ownership. **Start machines in maintenance mode** is not applicable for dedicated or floating instant clone pools. For details, see Manually Customizing Machines in an Automated Desktop Pool.
Dynamic or fixed pool size	Dynamic. If you remove a user assignment from a machine in a dedicated-assignment pool, the machine is returned to the pool of available machines. If you choose to delete machines on logoff in a floating-assignment pool, the pool size can grow or shrink depending on the number of active user sessions.	Fixed. The pool contains the number of machines you provide in the list of machine names. You cannot select the **Delete machine on logoff** setting if you name machines manually.

Table 11-3. Naming Machines Manually or Providing a Machine-Naming Pattern (continued)

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Spare machines	You can specify a number of spare machines that Horizon 8 keeps powered on for new users. Horizon 8 creates new machines to maintain the specified number. Horizon 8 stops creating spare machines when it reaches the maximum pool size. Horizon 8 keeps the spare machines powered on even when the pool power policy is **Power off** or **Suspend**, or when you do not set a power policy.	**Spare (Powered On) Machines** is not available for dedicated and floating instant clone pools when virtual machines are specified manually.
User assignment	You can use a naming pattern for dedicated-assignment and floating-assignment pools.	You can specify machine names for dedicated-assignment and floating-assignment pools. **Note** In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Specify a List of Machine Names

You can provision an automated desktop pool by manually specifying a list of machine names. This naming method lets you use your company's naming conventions to identify the machines in a pool.

When you explicitly specify machine names, users can see familiar names based on their company's organization when they log in to their remote desktops.

Follow these guidelines for manually specifying machine names:

- Type each machine name on a separate line.
- A machine name can have up to 15 alphanumeric characters.
- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are specified. The second machine is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com\jdoe
```

Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Make sure that each machine name is unique. You cannot use the names of existing virtual machines in vCenter Server.

Procedure

1 Create a text file that contains the list of machine names.

  If you intend to create a desktop pool with only a few machines, you can type the machine names directly in the **Add Pool** wizard. You do not have to create a separate text file.

2 In Horizon Console start the **Add Pool** wizard to begin creating an automated desktop pool that contains full virtual machines.

3 On the Provisioning Settings page, select **Specify names manually** and click **Enter names**.

4 Copy your list of machine names in the **Enter Machine Names** page and click **Next**.

5 Click **Submit**.

6 (Optional) Select **Start machines in maintenance mode**.

  This option lets you customize the machines before users can log in and use them.

7 Follow the prompts in the wizard to finish creating the desktop pool.

Results

Horizon 8 creates a machine for each name in the list. When an entry includes a machine and user name, Horizon 8 assigns the machine to that user.

After the desktop pool is created, you can add machines by importing another list file that contains additional machine names and users. See Add Machines to an Automated Pool Provisioned by a List of Names."

Add Machines to an Automated Pool Provisioned by a List of Names

To add machines to an automated desktop pool provisioned by manually specifying machine names, you provide another list of new machine names. This feature lets you expand a desktop pool and continue to use your company's naming conventions.

Follow these guidelines for manually adding machine names:

- Type each machine name on a separate line.

- The name must contain at least one alpha character.
- The name must contain only alphanumerics and dashes. Underscores are not allowed.
- The maximum length is 15 characters.
- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are added. The second machine is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Verify that you created the automated desktop pool of full virtual machines by manually specifying machine names. You cannot add machines by providing new machine names if you created the pool by providing a naming pattern.

Procedure

1 Create a text file that contains the list of additional machine names.

If you intend to add only a few machines, you can type the machine names directly in the **Add Pool** wizard. You do not have to create a separate text file.

2 In Horizon Console, select **Inventory > Desktops**.

3 Select the desktop pool to be expanded.

4 Click **Edit**.

5 Click the **Provisioning Settings** tab.

6 Click **Add Machines**.

7 Copy your list of machine names in the **Enter Machine Names** page and click **Next**.

8 Click **Submit**.

9 Click **OK**.

Results

In vCenter Server, you can monitor the creation of the new virtual machines.

In Horizon Console, you can view the machines as they are added to the desktop pool by selecting **Inventory > Desktops**.

Assign a Machine to a User in a Dedicated-Assignment Pool

In a dedicated-assignment pool, you can assign a user or multiple users to the virtual machine that hosts a remote desktop. Only the assigned user can log in and connect to the remote desktop. If a user is connected to session on a remote desktop, another user entitled to use the virtual machine cannot log in and connect to the remote desktop till the previous user logs off from the remote desktop.

Horizon Console assigns machines to users in these situations.

- When you create a dedicated-assignment desktop pool and select the **Enable automatic assignment** setting, Horizon Console automatically assigns machines to users.

  Note If you select the **Enable automatic assignment** setting, you can still manually assign machines to users.

- When you create an automated pool, select the **Specify names manually** setting, and provide user names with the machine names, Horizon Console automatically assigns machines to users.
- When you create a dedicated-assignment desktop pool and select the **Enable Multi-User Assignment** setting, you can manually assign multiple users to the same machine.

If you do not select either setting in a dedicated-assignment pool, users do not have access to virtual desktops. You must manually assign a machine to each user.

You can also use the `vdmadmin` command to assign machines to users. For more information about the `vdmadmin` command, see the *Horizon 8 Administration* guide.

Prerequisites

- Verify that the virtual machine belongs to a dedicated-assignment pool. In Horizon Console, the desktop pool assignment appears in the **User Assignment** column on the **Desktop Pools** page.

Procedure

1. In Horizon Console, select **Inventory > Desktops**, click a pool ID, and click the **Machines** tab.
2. Select the machine.
3. Select **Assign User(s)** from the **More Commands** drop-down menu.
4. Click **Add** and choose to select a domain, and type a search string in the **Name** or **Description** text box.
5. Select the user or users and click **Submit**.

What to do next

Navigate to **Users and Groups** to see the entitled users. After you assign a machine to a user or users and then navigate to **Users and Groups** and click **Find Machines** in the entitled group details, Connection Server searches and finds machines with assigned users for only those users and groups that belong to the same domain in the Active Directory group.

Unassign a User from a Dedicated Machine in Horizon Console

In a dedicated-assignment pool, you can remove a machine assignment to a user. If the dedicated-assignment pool is configured for multiple user assignment, you can remove a machine assignment for multiple users.

You can also use the `vdmadmin` command to remove a machine assignment to a user. For more information about the `vdmadmin` command, see the *Horizon 8 Administration* guide.

Procedure

1 In Horizon Console, select **Inventory > Desktops**, double-click a pool ID, and click the **Inventory** tab.

2 Select the machine.

3 Select **Unassign User(s)** from the **More Commands** drop-down menu and select the user or users that you want to remove from the machine assignment.

4 Click **OK**.

Results

The machine is available and can be assigned to another user.

Update Machine Aliases for Assigned Users

In a dedicated-assignment pool, you can update the aliases for assigned users to provide a custom desktop name to the end user.

Prerequisites

- Verify that the **Show Machine Alias Name** option is enabled in the desktop pool settings. See Worksheet for Creating an Instant-Clone Desktop Pool or Worksheet for Creating a Manual Desktop Pool .

Procedure

1 In Horizon Console, select **Inventory > Desktops**, select a pool, and click the **Machines** tab.

2 Select a machine.

3 Select **Update Machine Aliases** from the **More Commands** drop-down menu, and enter a machine alias.

4 Click **OK**.

Setting Power Policies for Desktop Pools

You can configure a power policy for the virtual machines in a desktop pool if the virtual machines are managed by vCenter Server.

Power policies control how a virtual machine behaves when its associated desktop is not in use. A desktop is considered not in use before a user logs in and after a user disconnects or logs off.

You configure power policies when you create or edit desktop pools in Horizon Console.

Note You cannot configure power policies for desktop pools that have non-vSphere machines.

Power Policies for Desktop Pools

Power policies control how a virtual machine behaves when the associated remote desktop is not in use.

You set power policies when you create or edit a desktop pool. Table 11-4. Power Policies describes the available power policies.

Table 11-4. Power Policies

Power Policy	Description
Take no power action	VMware Horizon 8 does not enforce any power policy after a user logs off. This setting has two consequences. ■ Horizon 8 does not change the power state of the virtual machine after a user logs off. For example, if a user shuts down the virtual machine, the virtual machine remains powered off. If a user logs off without shutting down, the virtual machine remains powered on. When a user reconnects to the desktop, the virtual machine restarts if it was powered off. ■ Horizon 8 does not enforce any power state after an administrative task is completed. For example, a user might log off without shutting down. The virtual machine remains powered on. When a scheduled recomposition takes place, the virtual machine is powered off. After the recomposition is completed, Horizon 8 does nothing to change the power state of the virtual machine. It remains powered off.
Always powered on	The virtual machine remains powered on, even when it is not in use. If a user shuts down the virtual machine, it immediately restarts. The virtual machine also restarts after an administrative task such as refresh, recompose, or rebalance is completed. Select **Always powered on** if you run batch processes or system management tools that must contact the virtual machines at scheduled times.
Suspend	The virtual machine enters a suspended state when a user logs off, but not when a user disconnects. You can also configure machines in a dedicated pool to be suspended when a user disconnects without logging off. To configure this policy, you must set an attribute in Horizon Directory. See Configure Dedicated Machines To Be Suspended After Users Disconnect. When multiple virtual machines are resumed from a suspended state, some virtual machines might have delays in powering on. Whether any delays occur depends on the ESXi host hardware and the number of virtual machines that are configured on an ESXi host. Users connecting to their desktops from Horizon Client might temporarily see a desktop-not-available message. To access their desktops, users can connect again. This policy is available for dedicated instant clone desktop pools created with NVIDIA GRID vGPU.
Power off	The virtual machine shuts down when a user logs off, but not when a user disconnects. This policy is not available for dedicated instant clone desktop pools created with NVIDIA GRID vGPU.

When you configure a full-clone desktop pool with floating assignments, the machine is not powered off even with the power policy set to **Power off** when the maximum number of machines is equal to the number of spare (power on) machines.

Note When you add a machine to a manual desktop pool, verify that the machine is powered on to ensure that it is fully configured, even when you select the **Power off** or **Take no power** action power policies. After Horizon Agent is configured, it is marked as **Ready**, and the normal power-management settings for the pool apply.

For manual desktop pools that contain vSphere virtual machines, a spare machine is always powered on so that users can connect to it. The spare machine is powered on no matter which power policy is in effect.

Table 11-5. When Horizon 8 Applies the Power Policy describes when Horizon 8 applies the configured power policy to full-clone desktop pools.

Table 11-5. When Horizon 8 Applies the Power Policy

Desktop Pool Type	The power policy is applied ...
Instant-clone desktop pool with dedicated assignment Instant-clone desktop pool that contains vSphere virtual machines with dedicated assignment	To dedicated virtual machines configured with default power policy set to **Always powered on**. On assigned machines, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned machine and are powered off or suspended when the user logs off. **Note** The **Always powered on** policy applies to assigned and unassigned machines.
Automated full-clone pool with dedicated assignment Manual desktop pool that contains vSphere virtual machines with dedicated assignment	To unassigned machines only. On assigned machines, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned machine and are powered off or suspended when the user logs off. **Note** The **Always powered on** policy applies to assigned and unassigned machines.
Automated full-clone pool with floating assignment Manual desktop pool that contains vSphere virtual machines with floating assignment	When a machine is not in use and after a user logs off. When you configure the **Power off** or **Suspend** power policy for a floating assignment desktop pool, set **Automatically logoff after disconnect** to **Immediately** to prevent discarded or orphaned sessions.
Manual desktop pool that contains one vSphere virtual machine with floating or dedicated assignment.	Power operations are initiated by session management. The virtual machine is powered on when a user requests an assigned machine and is powered off or suspended when the user logs off. **Note** The **Always powered on** policy applies to assigned and unassigned machines.

How Horizon 8 applies the configured power policy to automated pools depends on whether a machine is available. See How Power Policies Affect Automated Desktop Pools for more information.

Configure Dedicated Machines To Be Suspended After Users Disconnect

The **Suspend** power policy causes virtual machines to be suspended when a user logs off, but not when a user disconnects. You can also configure machines in a dedicated pool to be suspended when a user disconnects from a desktop without logging off. Using **Suspend** when users disconnect helps to conserve resources.

To enable suspend on disconnect for dedicated machines, you must set an attribute in Horizon Directory.

Procedure

1. Start the ADSI Edit utility on your Connection Server host.
2. In the console tree, select **Connect to**.
3. In the **Select or type a domain or server** field, type the server name as `localhost:389`
4. Under **Connection point**, click **Select or type a distinguished name or naming context**, type the distinguished name as `DC=vdi,DC=vmware,DC=int`, and click **OK**.

   The ADAM ADSI Edit main window appears.
5. Expand the ADAM ADSI tree and expand **OU=Properties**.
6. Select **OU=Global** and select **CN=Common** in the right pane
7. Select **Action > Properties**, and under the **pae-NameValuePair** attribute, add the new entry `suspendOnDisconnect=1`.
8. Restart the Connection Server service or Connection Server.

How Power Policies Affect Automated Desktop Pools

How VMware Horizon 8 applies the configured power policy to automated pools depends on whether a machine is available.

A machine in an automated pool is considered available when it meets the following criteria:

- Is active
- Does not contain a user session
- Is not assigned to a user

The Horizon Agent service running on the machine confirms the availability of the machine to Connection Server.

When you configure an automated pool, you can specify the minimum and maximum number of virtual machines that must be provisioned and the number of spare machines that must be kept powered on and available at any given time.

Power Policy Examples for Automated Pools with Floating Assignments

When you configure an automated pool with floating assignments, you can specify that a particular number of machines must be available at a given time. The spare, available machines are always powered on, no matter how the pool policy is set.

Power Policy Example 1

Table 11-6. Desktop Pool Settings for Automated Pool with Floating Assignment Example 1 describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 11-6. Desktop Pool Settings for Automated Pool with Floating Assignment Example 1

Desktop Pool Setting	Value
Number of machines (minimum)	10
Number of machines (maximum)	20
Number of spare, powered-on machines	2
Remote machine power policy	Power off

When this desktop pool is provisioned, 10 machines are created, two machines are powered on and immediately available, and eight machines are powered off.

For each new user that connects to the pool, a machine is powered on to maintain the number of spare, available machines. When the number of connected users exceeds eight, additional machines, up to the maximum of 20, are created to maintain the number of spare machines. After the maximum number is reached, the machines of the first two users who disconnect remain powered on to maintain the number of spare machines. The machine of each subsequent user is powered off according to the power policy.

Power Policy Example 2

Table 11-7. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2 describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 11-7. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2

Desktop Pool Setting	Value
Number of machines (minimum)	5
Number of machines (maximum)	5

Table 11-7. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2 (continued)

Desktop Pool Setting	Value
Number of spare, powered-on machines	2
Remote machine power policy	Power off

When this desktop pool is provisioned, five machines are created, two machines are powered on and immediately available, and three machines are powered off.

If a fourth machine in this pool is powered off, one of the existing machines is powered on. An additional machine is not powered on because the maximum of number of machines has already been reached.

Power Policy Example for Automated Pools with Dedicated Assignments

Unlike a powered-on machine in an automated pool with floating assignments, a powered-on machine in an automated pool with dedicated assignments is not necessarily available. It is available only if the machine is not assigned to a user.

Table 11-8. Desktop Pool Settings for Automated Pool with Dedicated Assignments Example describes the dedicated-assignment, automated pool in this example.

Table 11-8. Desktop Pool Settings for Automated Pool with Dedicated Assignments Example

Desktop Pool Setting	Value
Number of machines (minimum)	3
Number of machines (maximum)	5
Number of spare, powered-on machines	2
Remote machine power policy	Always powered on

When this desktop pool is provisioned, three machines are created and powered on. If the machines are powered off in vCenter Server, they are immediately powered on again, according to the power policy.

After a user connects to a machine in the pool, the machine becomes permanently assigned to that user. After the user disconnects from the machine, the machine is no longer available to any other user. However, the **Always powered on** policy still applies. If the assigned machine is powered off in vCenter Server, it is immediately powered on again.

When another user connects, a second machine is assigned. Because the number of spare machines falls below the limit when the second user connects, another machine is created and powered on. An additional machine is created and powered on each time a new user is assigned until the maximum machine limit is reached.

Preventing VMware Horizon 8 Power Policy Conflicts

When you use Horizon Console to configure a power policy, you must compare the power policy to the settings in the guest operating system's Power Options control panel to prevent power policy conflicts.

A virtual machine can become temporarily inaccessible if the power policy configured for the machine is not compatible with a power option configured for the guest operating system. If there are other machines in the same pool, they can also be affected.

The following configuration is an example of a power policy conflict:

- In Horizon Console, the power policy **Suspend** is configured for the virtual machine. This policy causes the virtual machine to enter a suspended state when it is not in use.
- In the Power Options control panel in the guest operating system, the option **Put the Computer to sleep** is set to three minutes.

In this configuration, both Connection Server and the guest operating system can suspend the virtual machine. The guest operating system power option might cause the virtual machine to be unavailable when Connection Server expects it to be powered on.

Configure Windows Desktop Session Timeouts in Horizon Console

You can specify timeout values for user inactivity and disconnected sessions on Windows desktops.

Procedure

- In the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor, enable these settings:

Setting	Properties
`Disconnect Session Time Limit (VDI)`	Specifies the amount of time after which a disconnected desktop session will automatically log off. ■ **Never**: disconnected sessions on this machine will never log off. ■ **Immediately**: disconnected sessions will immediately be logged off. You can also configure the time limit in the desktop pool setting **Automatically logoff after disconnect** in Horizon Console. If you configure this setting in both places, the GPO value takes precedence. For example, selecting **Never** here will prevent a disconnected session on this machine from ever logging off, regardless of what is set in Horizon Console.
`Idle Time Until Disconnect (VDI)`	Specifies the amount of time after which a desktop session will disconnect due to user inactivity. If disabled, unconfigured, or enabled with the setting **Never**, then the desktop sessions will never be disconnected. If the desktop pool or machine is configured to log off automatically after a disconnect, then that setting will be honored. The internal idle timer has a margin of error of 38 seconds. If you select 1 minute as the idle timeout, then the user will be disconnected automatically after 1 minute to 1 minute and 38 seconds of inactivity. If you select 5 minutes, then the user will be disconnected after 5 minutes to 5 minutes 38 seconds of inactivity.

Changes take effect the next time the user connects to the session.

For more information on group policy settings for Windows desktops, see VMware View Agent Configuration ADMX Template Settings in the *Horizon Remote Desktop Features and GPOs* document.

Managing Desktop Pools

You can perform administrative tasks on a desktop pool such as editing its properties, enabling, disabling, or deleting the pool.

Edit a Desktop Pool

You can edit an existing desktop pool to configure settings such as the number of spare machines, datastores, and customization specifications.

Prerequisites

Familiarize yourself with the desktop pool settings that you cannot change after a desktop pool is created. See Fixed Settings in an Existing Desktop Pool.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Select a desktop pool and click **Edit**.

3 Click a tab in the Edit dialog box and reconfigure desktop pool options.

4 Click **OK**.

Results

The desktop pool settings are updated.

If you change the image of an instant-clone desktop pool, the push image operation is invoked and the image publishing operation starts immediately. In Horizon Console, the summary page for the desktop pool shows the state for the pending image as `Publishing`.

If you change the cluster of an instant-clone desktop pool, new replica and golden image VMs are created in the new cluster. You can initiate a push image using the same image to have new clones created in the new cluster. However, the template VM, which is used in the cloning process, remains in the old cluster. You can put the ESXi host that the template VM is on in maintenance mode but you cannot migrate the template VM. To completely remove all infrastructure VMs including the template VM from the old cluster, you can initiate a push image using a new image.

Fixed Settings in an Existing Desktop Pool

After you create a desktop pool, you cannot change certain configuration settings.

Table 11-9. Fixed Settings in an Existing Desktop Pool

Setting	Description
Pool type	After you create an automated, manual, or RDS desktop pool, you cannot change the pool type.
User assignment	You cannot switch between dedicated assignments and floating assignments.
Type of virtual machine	You cannot switch between full virtual machines and instant-clone virtual machines.
Pool ID	You cannot change the pool ID.
vCenter settings	You cannot change vCenter Server settings for existing virtual machines. You can change vCenter Server settings in the Edit dialog box, but the values affect only new virtual machines that are created after the settings are changed.

Disable or Enable a Desktop Pool

When you disable a desktop pool, the pool is no longer presented to users and pool provisioning is stopped. Users have no access to the pool. After you disable a pool, you can enable it again.

Prerequisites

You can disable a desktop pool to prevent users from accessing their remote desktops while you prepare the desktops for use. If a desktop pool is no longer needed, you can use the disable feature to withdraw the pool from active use without having to delete the desktop pool definition from Horizon Console.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Select a desktop pool and change the status of the pool.

Option	Action
Disable the pool	Select **Disable Desktop Pool** from the **Status** drop-down menu.
Enable the pool	Select **Enable Desktop Pool** from the **Status** drop-down menu.

3 Click **OK**.

Disable or Enable Provisioning in a Desktop Pool

When you disable provisioning in an automated desktop pool, VMware Horizon 8 stops provisioning new virtual machines for the pool. After you disable provisioning, you can enable provisioning again.

Before you change a desktop pool's configuration, you can disable provisioning to ensure that no new machines are created with the old configuration. You also can disable provisioning to prevent Horizon 8 from using additional storage when a pool is close to filling up the available space.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Select a desktop pool and change the status of the pool.

Option	Action
Disable provisioning	Select **Disable Provisioning** from the **Status** drop-down menu.
Enable provisioning	Select **Enable Provisioning** from the **Status** drop-down menu.

3 Click **OK**.

Duplicate an Automated Desktop Pool

You can duplicate an automated desktop pool from an existing pool. When you duplicate a pool, the existing desktop pool's settings are copied into the duplicate desktop pool, allowing you to create a new pool without having to fill in each setting manually.

With this feature, you can streamline pool creation because you do not have to type every option in the wizard to add a desktop pool. You can ensure that desktop pool attributes are standardized by using the pre-filled values in the wizard.

You can duplicate automated desktop pools that contain full virtual machines or instant clones. You cannot duplicate manual desktop pools, or published desktop pools.

When you duplicate an instant-clone desktop pool that has the golden image virtual machine and its snapshot configured with NVIDIA Grid vGPU, the Suspend and Power Off power policies will not be available for selection in the duplicate pool wizard. Suspend and Power Off power policies will be available only when the selected golden image and its snapshot are not configured with NVIDIA Grid vGPU.

When you duplicate a full-clone desktop pool that has the virtual machine template configured with NVIDIA Grid vGPU, the Suspend power policy will not be available for selection in the duplicate pool wizard. Suspend power policy will be available only when the selected virtual machine template is not configured with NVIDIA Grid vGPU.

Prerequisites

- Verify that the prerequisites for creating the original desktop pool are still valid.

  When you clone a pool, you can use the same virtual machine template, a golden image virtual machine, or you can select another one.

Procedure

1. In Horizon Console, select **Inventory > Desktops**.
2. Select the desktop pool that you want to duplicate and click **Duplicate**.

   The **Duplicate Pool** wizard appears.

   Note You cannot change the settings for the desktop pool on the **Type**, **vCenter Server**, and **User Assignment** pages. You can modify settings on the other pages in the **Duplicate Pool** wizard.
3. To uniquely identify the duplicate desktop pool, on the **Desktop Pool Identification** page, type a unique pool ID.
4. On the **Provisioning Settings** page, provide unique names for the virtual machines.

Option	Description
Use a naming pattern	Type a virtual machine naming pattern.
Specify names manually	Provide a list of unique names for the virtual machines.

5. Click **Submit** or follow the other prompts in the wizard to complete and create the pool.

   Change desktop pool settings and values as needed.

Results

In Horizon Console, you can view the machines as they are added to the pool by selecting **Inventory > Desktops**.

What to do next

Entitle users to access the pool.

Delete a Desktop Pool

When you delete a desktop pool, users can no longer launch new remote desktops in the pool.

By default, you can delete a desktop pool even if desktop machines exist in the pool.

With an automated desktop pool of instant clones, VMware Horizon 8 always deletes the virtual machines from disk.

Important Do not delete the virtual machines in vvCenter Server before you delete a desktop pool with Horizon Console. This action could put Horizon 8 components into an inconsistent state.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Select a desktop pool and click **Delete**.

Results

Horizon 8 deletes all virtual machines from disk and terminates users' sessions to their remote desktops. On the **Desktops** page, the pool status appears as **Deleting**. It can take some time for Horizon 8 to delete the internal VMs from vCenter Server. Do not remove vCenter Server from Horizon Console until you verify that all the internal VMs are deleted.

Delete Virtual-Machine Desktops in a Pool

When you delete a virtual-machine desktop, users can no longer access the desktop.

Note Do not delete the virtual machines in vCenter Server before you delete virtual-machine desktops with Horizon Console. This action could put VMware Horizon 8 components into an inconsistent state.

Procedure

1 In Horizon Console, select **Inventory > Machines**

2 Select the **vCenter VMs** tab.

3 Select one or more machines and click **Remove**.

Results

vCenter Server deletes the instant-clone virtual machines from disk. Users in currently active sessions are disconnected from their remote desktops. With instant clones, vCenter Server always deletes the virtual machines from disk.

Note If you deleted a desktop pool in **Inventory > Desktops** the status of the desktop pool also appears as **Deleting** in **Inventory > Machines**.

Export VMware Horizon 8 Information to External Files

In Horizon Console, you can export Horizon 8 table information to external files. You can export the tables that list users and groups, pools, machines, events, and virtual desktop sessions. You can view and manage the information in a spreadsheet or another tool.

For example, you might collect information about machines that are managed by more than one Connection Server instance or group of replicated Connection Server instances. You can export the Machines table from each Horizon Console interface and view it in a spreadsheet.

When you export a Horizon Console table, it is saved as a Microsoft Excel Open XML Format Spreadsheet (XLSX) file. This feature exports the entire table, not individual pages.

Procedure

1. In Horizon Console, display the table you want to export.

   For example, click **Inventory > Machines** to display the machines table.
2. Click the export icon in the upper right corner of the table.

   When you point to the icon, the `Export table contents` tooltip appears.
3. Type a filename for the XLSX file in the Select location for download dialog box.
4. Browse to a location to store the file.
5. Click **Save**.

What to do next

Open a spreadsheet or another tool to view the XLSX format file.

Examining GPU Resources on an ESXi Host

To better manage the GPU resources that are available on an ESXi host, you can examine the current GPU resource reservation. The ESXi command-line query utility, `gpuvm`, lists the GPUs that are installed on an ESXi host and displays the amount of GPU memory that is reserved for each virtual machine on the host. Note that this GPU memory reservation is not the same as virtual machine VRAM size.

To run the utility, type **`gpuvm`** from a shell prompt on the ESXi host. You can use a console on the host or an SSH connection.

For example, the utility might display the following output:

```
~ # gpuvm
Xserver unix:0, GPU maximum memory 2076672KB
        pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
        pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
        GPU memory left 1684480KB.
```

Similarly, you can use the `nvidia-smi` command on the ESXi host to see a list of NVIDIA GRID vGPU-enabled virtual machines, the amount of frame buffer memory consumed, and the slot ID of the physical GPU that the virtual machine is using.

Creating Desktop Pools on a Single Host SDDC on VMware Cloud on AWS

VMware Cloud on AWS allows you to deploy a starter configuration containing a single host. The single host SDDC starter configuration is appropriate for test and development or proof of concept (PoC) use cases. VMware Horizon 8 supports creating full clones and instant clones on a single host SDDC for PoCs.

Do not run production workloads on a single host SDDC. Delete any desktop pools created for PoCs before scaling your SDDC to a full production SDDC.

For single host SDDC limitations, see "Deploying a Single Host SDDC Starter Configuration" in *VMware Cloud on AWS Product Documentation*.

Prevent Access to VMware Horizon 8 Desktops Through RDP

In certain Horizon 8 environments, it is a priority to prohibit access to Horizon 8 desktops through the RDP display protocol. You can prevent users and administrators from using RDP to access Horizon 8 desktops by configuring pool settings and a group policy setting.

By default, while a user is logged in to a remote desktop session, you can use RDP to connect to the virtual machine. The RDP connection terminates the remote desktop session, and the user's unsaved data and settings might be lost. The user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, deactivate the `AllowDirectRDP` setting.

Note Remote Desktop Services must be started on the virtual machine that you use to create pools and on the virtual machines that are deployed in the pools. Remote Desktop Services are required for Horizon Agent installation, SSO, and other Horizon 8 session-management operations.

Prerequisites

Verify that the Horizon Agent Configuration Administrative Template (ADMX) file is installed in Active Directory.

Procedure

1 Select the display protocol that you want Horizon Connection Server to use to communicate with Horizon Client devices.

Option	Description
Create a desktop pool	a In Horizon Console, start the **Add Pool** wizard. b On the Remote Display Protocol page, select **VMware Blast** or **PCoIP** as the default display protocol.
Edit an existing desktop pool	a In Horizon Console, select the desktop pool and click **Edit**. b On the **Desktop Pool Settings** tab, select **VMware Blast** or **PCoIP** as the default display protocol.

2 For the **Allow users to choose protocol** setting, select **No**.

3 Prevent devices that are not running Horizon Client from connecting directly to Horizon 8 desktops through RDP by disabling the `AllowDirectRDP` group policy setting.

   a On your Active Directory server, open the Group Policy Management Console and select **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware Horizon Agent Configuration**.

   b Disable the `AllowDirectRDP` setting.

Managing Storage for Virtual Desktops

12

Deploying desktops on virtual machines that are managed by vCenter Server provides all the storage efficiencies and capabilities enabled by vCenter Server. Using instant clones as desktop machines increases the storage savings because all virtual machines in a pool share a virtual disk with a base image.

Read the following topics next:

Managing Storage with VMware vSphere

vSphere lets you virtualize disk volumes and file systems so that you can manage and configure storage without having to consider where the data is physically stored.

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by vSphere to meet different data center storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

Instead of external arrays, you can use vSAN, which virtualizes the local physical solid-state disks and hard disk drives available on ESXi hosts into a single datastore shared by all hosts in a cluster. vSAN provides high-performance storage with policy-based management, so that you specify only one datastore when creating a desktop pool, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs).

vSAN also lets you manage virtual machine storage and performance by using storage policy profiles. If the policy becomes noncompliant because of a host, disk, or network failure, or workload changes, vSAN reconfigures the data of the affected virtual machines and optimizes the use of resources across the cluster.

Note vSAN is compatible with the View storage accelerator feature but not with the space-efficient disk format feature, which reclaims disk space by wiping and shrinking disks.

With vSphere, you can optionally use Virtual Volumes (vVols). This feature maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. This mapping allows vSphere to offload intensive storage operations such as snapshotting, cloning, and replication to the storage system.

Virtual Volumes also lets you manage virtual machine storage and performance by using storage policy profiles in vSphere. These storage policy profiles dictate storage services on a per-virtual-machine basis. This type of granular provisioning increases capacity utilization.

Note Virtual Volumes is compatible with the View storage accelerator feature but not with the space reclamation feature.

Note Instant clones do not support Virtual Volumes.

Using VMware vSAN for High-Performance Storage and Policy-Based Management

VMware vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of vSphere hosts. You specify only one datastore when creating an automated desktop pool or an automated farm, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs).

vSAN implements a policy-based approach to storage management. When you use vSAN, Horizon 8 defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles and automatically deploys them for virtual desktops onto vCenter Server. The policies are automatically and individually applied per disk (vSAN objects) and maintained throughout the life cycle of the virtual desktop. Storage is provisioned and automatically configured according to the assigned policies. You can modify these policies in vCenter Server. Horizon 8 creates vSAN policies for instant-clone desktop pools, full-clone desktop pools, or an automated farm per Horizon 8 cluster.

You can enable encryption for a vSAN cluster to encrypt all data-at-rest in the vSAN datastore. vSAN encryption is available with vSAN version 6.6 or later. For more information about encrypting a vSAN cluster, see the *VMware vSAN* documentation.

Each virtual machine maintains its policy regardless of its physical location in the cluster. If the policy becomes noncompliant because of a host, disk, or network failure, or workload changes, vSAN reconfigures the data of the affected virtual machines and load-balances to meet the policies of each virtual machine.

While supporting VMware vSphere features that require shared storage, such as HA, vMotion, and DRS, vSAN eliminates the need for an external shared storage infrastructure and simplifies storage configuration and virtual machine provisioning activities.

vSAN Workflow in Horizon 8

1. When creating an automated desktop pool or an automated farm in Horizon Console, under **Storage Policy Management**, select **Use VMware vSAN**, and select the vSAN datastore to use.

   After you select **Use VMware vSAN**, only the vSAN datastore is displayed.

   Default storage policy profiles are created according to the clone type you choose.

2. (Optional) Use vCenter Server to modify the parameters of the storage policy profiles, which include things like the number of failures to tolerate and the amount of SSD read cache to reserve. For specific default policies and values, see Default Storage Policy Profiles for VMware vSAN Datastores.

3. Use vCenter Server to monitor the vSAN cluster and the disks that participate in the datastore. For more information, see the *Administering VMware vSAN* document.

Requirements and Limitations

The vSAN feature has the following requirements and limitations when used in a Horizon 8 deployment:

- vSAN does not support VVOLs.
- vSAN is compatible with the View Storage Accelerator feature. vSAN provides a caching layer on SSD disks, and the View Storage Accelerator feature provides a content-based cache that reduces IOPS and improves performance during boot storms.
- Use appropriate hardware with vSAN. For specifics, see the VMware Compatibility Guide.
- Be mindful of cluster size and the vSAN maximum limit. For limits and recommendations from Horizon 8 onwards, see VMware Configuration Maximums.

Please see these additional resources to assist with planning:

- VMware Horizon on VMware vSAN Best Practices
- Horizon Active-Passive Service Using Stretched vSAN Cluster

Default Storage Policy Profiles for VMware vSAN Datastores

When you use vSAN, VMware Horizon 8 defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles, which you can modify. Storage is provisioned and automatically configured according to the assigned policies. The default policies that are created during desktop pool creation depend on the type of pool you create.

vSAN offers a storage policy framework so that you can control the behavior of various virtual machine objects that reside on the vSAN datastore. An example of an object in vSAN is a virtual disk (VMDK) file, and there are four characteristics of each object that are controlled through policy:

- **Stripes**: Number of disk stripes per object. The number of disk stripes affects how many magnetic disks you have (HDDs).
- **Resiliency**: Number of failures to tolerate. The number of host failures to tolerate depends, of course, on the number of hosts you have.
- **Storage Reservation**: Object space reservation. Controls how much storage is set aside.
- **Cache Reservation**: Flash read-cache reservation.

The stripes and cache reservation settings are used to control performance. The resiliency setting controls availability. The storage provisioning setting control capacity. These settings, taken together, affect how many VMware vSphere hosts and magnetic disks are required.

For example, if you set the number of disk stripes per object to 2, vSAN will stripe the object across at least 2 HDDs. In conjunction with this setting, if you set the number of host failures to tolerate to 1, vSAN will create an additional copy for resiliency and therefore require 4 HDDs. Additionally, setting the number of host failures to tolerate to 1 requires a minimum of 3 ESXi hosts, 2 for resiliency and the third to break the tie in case of partitioning.

Note If you are deploying Horizon 8 on VMware Cloud on AWS and require guidance on how to set the FTT value to meet the VMware Cloud on AWS SLA requirement, see the VMware Knowledge Base article https://kb.vmware.com/s/article/76366.

Table 12-1. Horizon Default Policies and Settings

Policy (as it appears in vCenter Server)	Description	Number of disk stripes per object	Number of failures to tolerate	Flash read-cache reservation	Object space reservation
`FULL_CLONE_DISK_<guid>`	Dedicated full-clone virtual disk	1	1	0	0
`FULL_CLONE_DISK_FLOATING_<guid>`	Floating full-clone virtual disk	1	0	0	0
`OS_DISK_FLOATING_<guid>`	Floating instant-clone OS and disposable disks	1	1	0	0

Table 12-1. Horizon Default Policies and Settings (continued)

Policy (as it appears in vCenter Server)	Description	Number of disk stripes per object	Number of failures to tolerate	Flash read-cache reservation	Object space reservation
`REPLICA_DISK_<guid>`	Instant-clone replica disk	1	1	0	0
`VM_HOME_<guid>`	VM home directory	1	1	0	0

Note <guid> indicates the UUID of the Horizon 8 cluster.

Once these policies are created for the virtual machines, they will never be changed by Horizon 8. An administrator can edit the policies created by Horizon 8 by going into vCenter Server through vSphere Client or the vSphere Command-Line Interface (`esxcli`), with the option to make the changes effective across all existing VMs or to any new VMs. Any new default policies enacted by Horizon 8 will not impact existing desktops pools. Each virtual machine maintains its policy regardless of its physical location in the cluster. If the policy becomes non-compliant because of a host, disk, network failure, or workload changes, vSAN reconfigures the data of the affected virtual machines and load-balances to meet the policies of each virtual machine.

Note If you inadvertently attempt to use settings that contradict each other, when you attempt to apply the settings, the operation will fail, and an error message might inform you that you do not have enough hosts.

Using Virtual Volumes for Virtual-Machine-Centric Storage and Policy-Based Management

With Virtual Volumes (VVols), an individual virtual machine, not the datastore, becomes a unit of storage management. The storage hardware gains control over virtual disk content, layout, and management. VMware Horizon 8 only supports VVols with full-clone virtual machines. Virtual Volumes datastores are not supported for instant clone desktop pools.

With Virtual Volumes, abstract storage containers replace traditional storage volumes based on LUNs or NFS shares. Virtual Volumes maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. With this mapping, VMware vSphere can offload intensive storage operations such as snapshotting, cloning, and replication to the storage system. The result, for example, is that a cloning operation that previously took an hour might now take a few minutes using Virtual Volumes.

Important One of the key benefits of Virtual Volumes is the ability to use Software Policy-Based Management (SPBM). However, Horizon 8 does not create the default granular storage policies that vSAN creates. Instead, you can set a global default storage policy in vCenter Server that applies to all Virtual Volume datastores.

Virtual Volumes has the following benefits:

- Virtual Volumes supports offloading a number of operations to storage hardware. These operations include taking snapshots, cloning, and Storage DRS.

- With Virtual Volumes, you can use advanced storage services that include replication, encryption, deduplication, and compression on individual virtual disks.
- Virtual Volumes supports such vSphere features as vMotion, Storage vMotion, snapshots, Flash Read Cache, and DRS.
- You can use Virtual Volumes with storage arrays that support vSphere APIs for Array Integration (VAAI).

Note Virtual Volumes is compatible with the View Storage Accelerator feature. vSAN provides a caching layer on SSD disks, and the View Storage Accelerator feature provides a content-based cache that reduces IOPS and improves performance during boot storms.

The Virtual Volumes feature has the following requirements:

- Appropriate hardware. Certain storage vendors are responsible for supplying storage providers that can integrate with vSphere and provide support for Virtual Volumes. Every storage provider must be certified by VMware and properly deployed.
- All virtual disks that you provision on a virtual datastore must be an even multiple of 1 MB.

Virtual Volumes is a vSphere feature. For more information about the requirements, functionality, background, and setup requirements, see the topics about Virtual Volumes in the *vSphere Storage* document.

Reducing Storage Requirements with Instant Clones

Instant clones leverage VMware vSphere vmFork technology to quiesce a running base image, or parent VM, and rapidly create and customize a pool of virtual desktops.

Instant clones share the virtual disks with the parent VM at the time of creation. Each instant clone acts like an independent desktop with a unique host name and IP address, yet the instant clone requires significantly less storage. Instant clones reduce the required storage capacity by 50 to 90 percent.

Storage for Instant Clones

Instant clones support the use of all standard vSphere storage options: VMFS, NFS, vSAN, and local datastores.

You can store instant clones on spinning media-backed (HDDs) datastores or on datastores backed by solid-state drives (SSDs). HDDs provide lower performance, but are less expensive and provide higher storage capacity. SSDs have low storage capacity and high read performance, typically supporting tens of thousands of I/Os per second (IOPS).

One way to lower the storage cost is through the tiered use of HDDs and SSDs. When you create an instant-clone desktop pool, VMware Horizon 8 creates a series of internal VMs for managing instant clones. One such internal VM is a replica, which is essentially a full clone made from the golden image. The replica and the subsequent instant clones made from it can be placed on the same datastore/LUN (logical unit number), or separate datastores with different performance characteristics. For example, you can store the replica VMs on a SSD-backed datastore. A typical environment has only a small number of replica VMs, so replicas do not require much storage. You can then store instant clones on HDDs. They are inexpensive and provide high storage capacity, which makes them suited for storing a large number of clones.

Configuring replicas and clones in this way can reduce the impact of I/O storms that occur when many clones are created at once. For example, if you deploy a floating-assignment pool with a delete-machine-on-logoff policy, and your users start work at the same time, Horizon 8 must concurrently provision new machines for them.

Important This feature is designed for specific storage configurations provided by vendors who offer high-performance disk solutions. Do not store replicas on a separate datastore if your storage hardware does not support high-read performance.

You must follow certain requirements when you store the replica and clones in a pool on separate datastores:

- You can specify only one separate replica datastore for a pool.
- The replica datastore must be accessible from all ESXi hosts in the cluster.
- This feature is not available if you use vSAN datastores. These types of datastores use Software Policy-Based Management, so that storage profiles define which components go on which types of disks.

Availability Considerations for Storing Replicas on a Separate Datastore

You can store replica VMs on a separate datastore or on the same datastores as the clones. These configurations affect the availability of the pool in different ways.

When you store replicas on the same datastores as the clones to enhance availability, a separate replica is created on each datastore. If a datastore becomes unavailable, only the clones on that datastore are affected. Clones on other datastores continue to run.

When you store replicas on a separate datastore, all clones in the pool are anchored to the replicas on that datastore. If the datastore becomes unavailable, the entire pool is unavailable.

To enhance the availability of the desktop pool, you can configure a high-availability solution for the datastore on which you store the replicas.

Using Persistent Disks for Dedicated Windows Instant Clones

Persistent disks on dedicated instant clones allow the flexibility of storing user settings and other user-generated data on a disk independent of the VM.

Persistent Disk is a feature that existed on View Composer linked clones, which were deprecated in Horizon 8. Persistent disks are used as a secondary disk to store OS data and user information on virtual machines when the OS data is updated, refreshed, or rebalanced. Persistent disks are their own managed objects and are maintained without being tied to a particular VM, allowing VMware administrators the flexibility to set up persistent disks according to their needs, attaching to a VM and detaching from the VM when needed. All datastores support persistent disks.

Consider these guidelines and persistent disk behavior when creating and managing persistent disks:

- The persistent disk feature is available for dedicated desktops only.
- Persistent disks are not available for Linux based virtual machines as this feature uses Windows specific APIs.
- Persistent disks do not support a multi-user assignment.
- A desktop can have one primary persistent disk and zero to at least one secondary persistent disk.
- A secondary disk is similar to a primary disk and can be used to expand the storage capacity for a few users in a pool or give access to other users' primary disk to an admin or supervisor in case an employee moves out of the organization.
- Creating a pool with persistent disks:
  - You can create a desktop pool with a primary persistent disk in the instant clone desktop pool creation workflow.
  - When creating a pool with a persistent disk, you must specify a drive letter for the persistent disk and storage capacity in megabytes. Windows will redirect the user profile to this drive to store user information.
- Editing a pool with persistent disks:
  - You can edit a persistent disk in the edit instant clone desktop pool workflow.
  - You can change the drive letter and the size of the persistent disk.
  - When you change the drive letter of the persistent disk, only the new desktops created will have the new drive letter.
- Deleting a pool with persistent disks:
  - When you delete an entire desktop pool, the underlying persistent disks including any secondary disks are also deleted.
  - If you want to retain the persistent disks, you must detach all the disks before deleting the pool.
- After the pool with persistent disks is created, VMware recommends that you add user or group entitlements to the desktop pool so that the persistent disk is associated with a user.

- For persistent disks to work successfully, the golden image VM must have a SCSI controller configured and present, as well as a device, such as a main hard disk, configured on the SCSI controller.

If you are using persistent disks with dedicated linked clones in a Horizon 7.x environment, consult this migration guidance on how you can move to Horizon 8 and continue to use persistent disks with dedicated instant clones: https://kb.vmware.com/kb/93091

For best practices and troubleshooting, see https://kb.vmware.com/kb/92881.

Attach a Persistent Disk to a Windows Instant Clone

You can attach a persistent disk to a Windows instant clone virtual machine. Attaching a persistent disk makes the user settings and information in the disk available to the user of the other virtual machine.

You can select a detached persistent disk and attach it to an instant clone VM from a pool that has persistent disk enabled and a user is assigned to the VM to which a persistent disk will be attached. An attached persistent disk will become available as a secondary disk on the selected instant-clone virtual machine. You can attach more than one secondary disk to an instant clone desktop.

Prerequisites

- Before you attach a persistent disk to another VM, make sure you have a pool with persistent disk created and users are assigned to the VMs of this pool.
- You cannot attach a persistent disk that is stored on a non-vSAN datastore to a virtual machine that is stored on a vSAN datastore. Similarly, you cannot attach a disk that is stored on vSAN to a virtual machine that is stored on non-vSAN. Horizon Console prevents you from selecting virtual machines that span vSAN and non-vSAN datastores.
- Persistent disks are not available for Linux based virtual machines as this feature uses Windows specific APIs.
- Persistent disks must be reconnected to the operating system that was used when they were created. For example, you cannot detach a persistent disk from a Windows 7 instant clone and recreate or attach the persistent disk to a Windows 8 instant clone.

Procedure

1. In Horizon Console, select **Inventory > Persistent Disks**.
2. On the **Detached** tab, select the persistent disk and click **Attach**.
3. In the pop-up window displaying the list of machines, select the machine with its corresponding user and desktop pool, and click **Attach**.

   Note Filtering and sorting for the attachable-machines grid is not currently supported.

What to do next

Verify that the user of the instant clone has sufficient privileges to use the attached disk. For example, if the original user had certain access permissions on the persistent disk, and the persistent disk is attached as drive `D` on the new linked clone, the new user of the instant clone must have the original user's access permissions on drive `D`.

Log in to the instant clone's guest operating system as an administrator and assign appropriate privileges to the new user.

Detach a Persistent Disk

When you detach a persistent disk, the disk is stored and the instant clone is deleted. By detaching a persistent disk, you can store and reuse user-specific information with another virtual machine.

A detached disk is stored in the current datastore. Detaching a secondary persistent disk does not result in the deletion of the instant clone desktop.

Prerequisites

A user must be assigned to the desktop to detach a persistent disk.

Procedure

1 In Horizon Console, select **Inventory > Persistent Disks**.

2 In the **Attached** tab, select the persistent disk with a user assigned and click **Detach**

Results

After detaching, the status changes to `Detach Persistent Disk`. The instant clone associated with the disk is deleted and the persistent disk appears in the detached section.

Recreate a Windows Instant Clone With a Detached Persistent Disk

When you detach a persistent disk, the Windows-based instant clone is deleted. You can give the original user access to the detached user settings and information by recreating the instant clone virtual machine from the detached disk.

Note If you recreate an instant clone virtual machine in a desktop pool that has reached its maximum size, the recreated virtual machine is still added to the desktop pool. The desktop pool size grows and then reduces as unassigned machines are deleted.

Horizon 8 does not support recreating a virtual machine with a persistent disk that is stored on a non-vSAN datastore if the new virtual machine is stored on a vSAN datastore. Similarly, if the persistent disk is stored on vSAN, Horizon 8 does not support recreating a virtual machine on non-vSAN.

To move a detached persistent disk from non-vSAN to vSAN, you can recreate the disk on a virtual machine that is stored on a non-vSAN datastore and rebalance the virtual machine's desktop pool to a vSAN datastore.

Procedure

1 In Horizon Console, select **Inventory > Persistent Disks**.

2 On the **Detached** tab, select the persistent disk, and click **Recreate Machine**.

  You can select multiple persistent disks to recreate an instant clone virtual machine for each disk.

3 Click **OK**.

Results

Horizon 8 creates an instant clone virtual machine for each persistent disk you select and adds the virtual machine to the original desktop pool.

The persistent disks remain on the datastore where they were stored.

Storage Sizing for Instant-Clone Desktop Pools

VMware Horizon 8 provides high-level guidelines that can help you determine how much storage an instant-clone desktop pool requires.

During the instant clone pool creation process, Horizon 8 displays a storage-sizing table with the free space on the datastores that you select for storing OS disks. You can decide which datastores to use by comparing the actual free space with the estimated requirements for the desktop pool. The formulas used in the table only provide a general estimate of storage use. The clones' actual storage growth depends on many factors:

- Amount of memory assigned to the golden image.
- Size of the guest operating system's paging file.
- Workload on the desktop machines, determined primarily by the types of applications that users run in the guest operating system.

Note In a deployment that includes hundreds or thousands of clones, configure your desktop pool so that particular sets of datastores are dedicated to particular ESXi clusters. Do not configure pools randomly across all the datastores so that most or all ESXi hosts must access most or all LUNs.

When too many ESXi hosts attempt to write to the OS disks on a particular LUN, contention problems can occur, degrading performance and interfering with scalability. For more information about datastore planning in large deployments, see the *Horizon Overview and Deployment Planning* document.

Storage Sizing Guidelines for Instant-Clone Desktop Pools

When you create or edit an instant-clone desktop pool, the **Select Instant Clone Datastores** page displays a table that provides storage-sizing guidelines. The table can help you to decide which datastores to select for the instant-clone disks. The guidelines calculate space needed for new clones.

Sizing Table for OS Disks

Example Sizing Table for OS Disks shows an example of storage-sizing recommendations that might be displayed for a pool of 10 virtual machines if the golden image virtual machine has 1GB of memory and a 10GB replica.

Table 12-2. Example Sizing Table for OS Disks

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	40.00	80.00	130.00

The **Selected Free Space** column shows the total available space on all of the datastores that you selected for a disk type such as OS disks.

The **Min Recommended** column shows the minimum amount of recommended storage for a pool.

The **50% Utilization** column shows the recommended storage when the disks grow to 50% of the golden image.

The **Max Recommended** column shows the recommended storage when the disks approach the full size of the golden image.

VMware Horizon 8 estimates the storage space that is needed for new clones. When you create a desktop pool, the sizing guidelines encompass the entire pool. When you edit an existing desktop pool, the guidelines encompass only the new clones that you add to the pool.

For example, if you add 100 clones to a desktop pool and select a new datastore, Horizon 8 estimates space requirements for the 100 new clones. If you select a new datastore but keep the desktop pool the same size, or reduce the number of clones, the sizing guidelines show 0. The value of 0 reflect that no new clones must be created on the selected datastore. Space requirements for the existing clones are already accounted for.

How Horizon 8 Calculates the Minimum Sizing Recommendations

To arrive at a minimum recommendation for OS disks, Horizon 8 estimates that each clone consumes twice its memory size when it is first created and started up. If no memory is reserved for a clone, an ESXi swap file is created for a clone as soon as it is powered on. The size of the guest operating system's paging file also affects the growth of a clone's OS disk.

In the minimum recommendation for OS disks, Horizon 8 also includes space for two replicas on each datastore. Horizon 8 creates one replica when a pool is created. When the instant-clone pool is patched for the first time by a push image, Horizon 8 creates a second replica on the datastore, anchors the clones to the new replica, and deletes the first replica if no other clones are using original snapshot. The datastore must have the capacity to store two replicas during the recompose operation.

By default, replicas use VMware vSphere thin provisioning, but to keep the guidelines simple, Horizon 8 accounts for two replicas that use the same space as the golden image virtual machine.

To arrive at a minimum recommendation storing replicas on a separate datastore, Horizon 8 allows space for two replicas on the datastore. The same value is calculated for minimum and maximum usage.

For details, see Storage Sizing Formulas for Instant-Clone Desktop Pools.

Storage Sizing Formulas for Instant-Clone Desktop Pools

Storage-sizing formulas can help you estimate how much disk space is required on the datastores that you select for OS disks and replicas.

Storage Sizing Formulas

Storage Sizing Formulas for Clone Disks on Selected Datastores shows the formulas that calculate the estimated sizes of the disks when you create a pool and as the clones grow over time. These formulas include the space for replica disks that are stored with the clones on the datastore.

If you edit an existing pool or store replicas on a separate datastore, VMware Horizon 8 uses a different sizing formula. See Storage Sizing Formulas for Creating Instant Clones When You Edit a Pool or Store Replicas on a Separate Datastore.

Table 12-3. Storage Sizing Formulas for Clone Disks on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of VMs * (2 * memory of VM) + (2 * replica disk)	Number of VMs * (50% of replica disk + memory of VM) + (2 * replica disk)	Number of VMs * (100% of replica disk + memory of VM) + (2 * replica disk)

Example of a Storage Sizing Estimate

In this example, the golden image is configured with 1GB of memory. The golden image's disk size is 10GB. A pool is created with 10 machines.

The OS disks are configured on a datastore that currently has 184.23GB of available space.

Example of a Sizing Estimate for Clone Disks Deployed on Selected Datastores shows how the sizing formulas calculate estimated storage requirements for the sample desktop pool.

Table 12-4. Example of a Sizing Estimate for Clone Disks Deployed on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) + (2*10GB) = 40.00	10 * (50% of 10GB + 1GB) + (2*10GB) = 80.00	10 * (100% of 10GB + 1GB) + (2*10GB) = 130.00

Storage Sizing Formulas for Creating Instant Clones When You Edit a Pool or Store Replicas on a Separate Datastore

VMware Horizon 8 calculates different sizing formulas when you edit an existing desktop pool, or store replicas on a separate datastore, than when you first create a pool.

If you edit an existing pool and select datastores for the pool, Horizon 8 creates new clones on the selected datastores. The new clones are anchored to the existing snapshot and use the existing replica disk. No new replicas are created.

Horizon 8 estimates the sizing requirements of new clones that are added to the desktop pool. Horizon 8 does not include the existing clones in the calculation.

If you store replicas on a separate datastore, the other selected datastores are dedicated to the OS disks.

The following table shows the formulas that calculate the estimated sizes of clone disks when you edit a pool or store replicas on a separate datastore.

Table 12-5. Storage Sizing Formulas for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of new VMs * (2 * memory of VM)	Number of new VMs * (50% of replica disk + memory of VM)	Number of new VMs * (100% of replica disk + memory of VM)

Example of a Storage Sizing Estimate When You Edit a Pool or Store Replicas on a Separate Datastore

In this example, the golden image virtual machine is configured with 1GB of memory. The golden image virtual machine's disk size is 10GB. A pool is created with 10 machines.

The OS disks are configured on a datastore that currently has 184.23GB of available space.

The following table shows how the sizing formulas calculate estimated storage requirements for the sample pool.

Table 12-6. Example of a Sizing Estimate for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) = 20.00	10 * (50% of 10GB + 1GB) = 60.00	10 * (100% of 10GB + 1GB) = 110.00

Storing Instant Clones on Local Datastores (non-VMware vSAN)

Instant-clone virtual machines can be stored on local datastores, which are internal spare disks on ESXi hosts. Local storage offers advantages such as inexpensive hardware, fast virtual-machine provisioning, high performance power operations, and simple management. However, using local storage limits the VMware vSphere infrastructure configuration options that are available to you. Using local storage is beneficial in certain VMware Horizon 8 environments but not appropriate in others. Only NVMe, SAS or SATA drives are supported.

Note The limitations described in this topic do not apply to vSAN datastores, which also use local storage disks but turns them into shared storage.

Using local datastores is most likely to work well if the Horizon 8 desktops in your environment are non-persistent. For example, you might use local datastores if you deploy kiosks or classroom and training stations.

Consider using local datastores if your virtual machines have floating assignments, are not dedicated to individual end users, do not require persistent disks for user data, and can be deleted or refreshed at regular intervals such as on user logoff. This approach lets you control the disk usage on each local datastore without having to move or load-balance the virtual machines across datastores.

However, you must consider the restrictions that using local datastores imposes on your Horizon 8 desktop or farm deployment:

- You cannot use VMotion.
- You cannot use VMware vSphere High Availability.
- You cannot use the vSphere Distributed Resource Scheduler (DRS).
- If you are deploying instant clones on a single ESXi host with a local datastore, you must configure a cluster containing that single ESXi host. If you have a cluster of two or more ESXi hosts with local datastores, select the local datastore from each of the hosts in the cluster. Otherwise, instant clone creation fails.
- Local spinning-disk drives and a storage array might have similar capacity, but local spinning-disk drives do not have the same throughput as a storage array. Throughput increases as the number of spindles grows. If you select direct attached solid-state disks (SSDs), performance is likely to exceed that of many storage arrays. Local datastore support for instant clones is available for both virtual desktops and published desktops

Configure View Storage Accelerator for Desktop Pools

You can enable View Storage Accelerator on pools that contain instant clones and on pools that contain full-clone virtual machines. This feature uses the Content Based Read Cache (CBRC) feature in ESXi hosts.

CBRC uses ESXi host memory to cache virtual machine disk data, reduce IOPS, and improve performance during boot storms, when many machines start up or run anti-virus scans at once. By reducing the number of IOPS during boot storms, View Storage Accelerator lowers the demand on the storage array, which lets you use less storage to support your Horizon 8 deployment. The feature is also beneficial when administrators or users load applications or data frequently.

When a virtual machine is created, Horizon 8 indexes the contents of each virtual disk file. The indexes are stored in a virtual machine digest file. At runtime, the ESXi host reads the digest files and caches common blocks of data in memory. To keep the ESXi host cache up to date, Horizon 8 regenerates the digest file at regular intervals. You can modify the regeneration interval.

Native NFS snapshot technology (VAAI) and Vvols are not supported in pools that are enabled for View Storage Accelerator. vSphere VM Encryption is also not supported with View Storage Accelerator.

To enable the View Storage Accelerator feature, you must enable it globally and then enable it for individual desktop pools. For details on how to enable or disable View Storage Accelerator globally, see the *Horizon 8 Installation and Upgrade* document.

After View Storage Accelerator is enabled globally, you can enable or disable it for individual full-clone desktop pools. For instant-clone desktop pools, View Storage Accelerator is only needed for replica VMs and is enabled automatically for individual pools. It cannot be turned off on a pool level. To disable, you must disable View Storage Accelerator globally, and this step will also disable the feature for full clone pools.

Note Disabling View Storage Accelerator globally will not change the existing instant clone pool. The new instant clone pool still needs to be deployed.

View Storage Accelerator is enabled for a full-clone pool by default. The feature can be disabled or enabled when you create or edit a pool. The best approach is to enable this feature when you first create a desktop pool.

Procedure

1 In Horizon Console, display the **Advanced Storage Options** tab in the pool creation wizard.

Option	Description
New desktop pool (recommended)	Start the Add Pool wizard to begin creating an automated desktop pool. Follow the wizard configuration prompts until you reach the **Advanced Storage Options** page.
Existing desktop pool	Select the existing pool, click **Edit**, and click the **Advanced Storage Options** tab. If you modify View Storage Accelerator settings for an existing desktop pool, the changes do not take effect until the virtual machines in the desktop pool are powered off.

2 To enable View Storage Accelerator for the pool, make sure that the **Use View Storage Accelerator** check box is selected.

This setting is selected by default. To disable the setting, uncheck the **Use View Storage Accelerator** box. You cannot select a disk type. View Storage Accelerator is performed on the whole virtual machine.

3 (Optional) In the **Regenerate storage accelerator after** text box, specify the interval, in days, after which the regeneration for View Storage Accelerator digest files take place.

The default regeneration interval is seven days.

What to do next

You can configure blackout days and times during which disk space reclamation and View Storage Accelerator regeneration do not take place. See Set Storage Accelerator and Space Reclamation Restriction Times.

Reclaim Disk Space on Instant Clones

The disk space reclamation feature is for longer-lived instant clones.

Instant clones can be either short-lived or longer-lived. Short-lived instant clones are clones created with floating assignment or dedicated assignment with the **Refresh on Logoff** set to **Always**. Short-lived instant clones are deleted and then recreated whenever a user logs out. Because of the frequent refresh of short-lived instant clones, the clones' OS disks do not get much chance to grow unlike the OS disks for longer-lived instant clones, so it is beneficial to allow ESXi hosts to reclaim unused disk space, thereby reducing the total storage space required.

VMware Horizon 8 creates all instant clone virtual machines in an efficient disk format. As users interact with instant clone desktops, the clones' OS disks grow and can eventually use almost as much disk space as full-clone desktops. Disk space reclamation reduces the size of the OS disks. Space can be reclaimed while the virtual machines are powered on and users are interacting with their remote desktops. With disk space reclamation, Horizon 8 can maintain instant clones at close to the reduced size they start out with when they are first provisioned.

Space reclamation works differently depending on whether you are using a VMware vSAN or non-vSAN datastore, and for the specific version of VMware vSphere and vSAN you are running:

- On vSAN storage, there is no support for space reclamation prior to vSphere/vSAN 6.7U1.
- Starting from vSphere/vSAN 6.7U1, space reclamation is supported via the vCenter Server TRIM and UNMAP feature on vSAN datastores.
- On non-vSAN storage, prior to vSphere 6.7, Horizon 8 implements a periodic space reclamation operations.
- On non-vSAN storage, from vSphere version 6.7 and later, VMFS-6 supports the Automatic UNMAP feature, which reclaims dead blocks automatically and asynchronously if it is not turned off by the vSphere or vCenter Server administrator. Therefore, you no longer need to enable the manual process on Horizon 8.

Disk space reclamation is not applicable for full clones. For more details, see the *Horizon 8 Installation and Upgrade* document.

Enable Periodic Space Reclamation for VMware vSphere 6.7 and Earlier on Non-vSAN Datastores

This task is relevant if you are using a vSphere version earlier than 6.7 on non-vSAN datastores.

Enabling periodic space reclamation on VMware Horizon 8 is a two-step process.

- You must enable or deactivate space reclamation globally for each vCenter Server. You can configure space reclamation in Horizon Console by navigating to **Settings > Servers**. You can deactivate this feature on all desktop pools that are managed by the vCenter Server instance. Deactivating the feature at this level overrides the setting at the desktop pool level.
- After you enable space reclamation globally, you can enable or deactivate space reclamation at individual pool level.

Prerequisites

Verify the following prerequisites for individual desktop pools.

- Verify that the golden image has virtual hardware version 9 or later.
- Verify that the storage for the pool uses SCSI controllers. Disk space reclamation is not supported on virtual machines with IDE controllers.
- Verify that disk space reclamation is enabled in globally. This option ensures that the virtual machines in the pool are created in the efficient disk format that is required to reclaim disk space. It is available for instant clones and recommended for longer lived instant clone pools where the desktop is never refreshed on user logout. For other types of instant clones, the benefit from space reclamation may be insignificant.

Procedure

1 Complete these steps to set up space reclamation globally.

   a In Horizon Console, navigate to **Settings > Servers**.

   b On the **vCenter Server** tab, click **Add**, and navigate to the **Storage Settings** page.

   c On the **Storage Settings** page, select **Reclaim VM Disk Space**.

   This option is selected by default if you perform a fresh installation of Horizon 8. You must select this option if you upgrade to a later release of Horizon 8.

2 Complete these steps to set up space reclamation for individual desktop pools.

   a In Horizon Console, navigate to the **Desktop Pool Settings** page of the instant clone pool creation wizard.

   b Select the **Reclaim VM disk space** check box.

   c In the **Initiate reclamation when unused space on VM exceeds** text box, type the minimum amount of unused disk space, in gigabytes, that must accumulate on an instant clone OS disk before ESXi starts reclaiming space on that disk.

   For example: **2** GB.

   The default value is 1 GB.

What to do next

You can configure restricted days and times during which disk space reclamation and regeneration for View Storage Accelerator do not take place. See Set Storage Accelerator and Space Reclamation Restriction Times.

In Horizon Console, you can select **Inventory > Desktops** and select a machine to display the last time space reclamation occurred and the last amount of space reclaimed on the machine.

You can use the `vdmadmin -M`option to initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes. See the *Horizon 8 Administration* document.

Reclaiming Disk Space for VMware vSphere 6.7 and Later on Non-vSAN Datastores

This topic is relevant if you are using vSphere 6.7 and later, on non-vSAN datastores. In vSphere version 6.7 and later, VMFS-6 supports the Automatic UNMAP feature, which reclaims dead blocks automatically and asynchronously (if it is not deactivated by the vSphere or vCenter Server administrator). Therefore, the periodic space reclaim operations by VMware Horizon 8 do not reclaim significant space.

In Horizon Console, the option **Space reclaimed in the latest run over the last 7 days** typically shows a value of 0.00 GB, since this is an indication of the specific Horizon 8 periodic space reclamation operations.

Unless you have deactivated automatic UNMAP feature on vSphere or vCenter, no action is needed on Horizon 8 to reclaim space.

Reclaim Disk Space for VMware vSphere 6.7U1 and later on vSAN datastores

This topic is relevant if you are using vSAN datastores. Prior to vSphere with vSAN 6.7U1, there is no space reclamation support. Starting with 6.7U1, vSAN space reclamation is supported with the vCenter Server UNMAP feature on vSAN datastores. It is deactivated by default.

Procedure

1 Check that the UNMAP feature is enabled in the ESXi host.

   Run the following commands from the command line:

   ```
   esxcfg-advcfg -g /VSAN/GuestUnmap
   ```

   The value of the "GuestUnmap" option is 0.

   ```
   esxcfg-advcfg -g /VSAN/Unmap
   ```

   The value of the "Unmap" option is 1.

2 Enable guest UNMAP in all ESXi hosts.

   Run the following command:

   ```
   esxcfg-advcfg -s 1 /VSAN/GuestUnmap
   ```

   Then, check the UNMAP feature for the guest operating system. Run the following command:

   ```
   esxcfg-advcfg -g /VSAN/GuestUnmap
   ```

   The value of the GuestUnmap option is 1.

3 Enable the UNMAP feature in vCenter Server.

   Run the following RVC command:

   ```
   vsan.unmap_support <cluster> -e
   ```

Set Storage Accelerator and Space Reclamation Restriction Times

Regenerating digest files for View Storage Accelerator and reclaiming virtual machine disk space can use ESXi resources. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days.

For example, you can specify a restriction period during weekday morning hours when users start work, and boot storms and anti-virus scanning I/O storms take place. You can specify different restriction times on different days.

Disk space reclamation and View Storage Accelerator digest file regeneration do not occur during restriction times that you set. You cannot set separate restriction times for each operation.

Horizon 8 allows View Storage Accelerator digest files to be created for new machines during the provisioning stage, even when a restriction time is in effect.

Note The following procedure applies to full-clone desktop pools only.

Prerequisites

- Verify that **Enable View Storage Accelerator**, **Enable space reclamation**, or both features are selected for vCenter Server.
- Verify that **Use View Storage Accelerator**, **Reclaim VM disk space**, or both features are selected for the desktop pool.

Procedure

1 On the **Advanced Storage Options** page in the Add Pool wizard, go to **Blackout Times** and click **Add**.

  If you are editing an existing pool, click the **Advanced Storage Options** tab.

2 Check the restriction days and specify the starting and ending times.

  The time selector uses a 24-hour clock. For example, 10:00 is 10:00 a.m., and 22:00 is 10:00 p.m.

3 Click **OK**.

4 To add another restriction period, click **Add** and specify another period.

5 To modify or remove a restriction period, select the period from the Blackout times list and click **Edit** or **Remove**.

Monitoring Virtual Desktops and Desktop Pools

13

You can use Horizon Console to monitor the status of virtual desktops, unmanaged machines, or the status of vCenter Server virtual machines in your VMware Horizon 8 deployment.

Read the following topics next:

- Monitor Virtual-Machine Desktop Status
- Status of vCenter Server Virtual Machines
- Recover Instant-Clone Desktops
- Status of Unmanaged Machines

Monitor Virtual-Machine Desktop Status

You can quickly survey the status of virtual-machine desktops in your VMware Horizon 8 deployment by using the Horizon Console dashboard. For example, you can display all disconnected virtual machines or virtual machines that are in maintenance mode.

Prerequisites

Familiarize yourself with the virtual machine states. See Status of vCenter Server Virtual Machines.

Procedure

1. In Horizon Console, click **Dashboard**.
2. In the Machine Status pane, expand a status folder.

Option	Description
Preparing	Lists the machine states while the virtual machine is being provisioned, deleted, or in maintenance mode.
Problem Machines	Lists the machine error states.
Prepared for use	Lists the machine states when the virtual machine is ready for use.

3. Locate the machine status and click the hyperlinked number next to it.

Results

The Machines page displays all virtual machines with the selected status.

What to do next

You can click a machine name to see details about the virtual machine or click the Horizon Console back arrow to return to the dashboard page.

Status of vCenter Server Virtual Machines

Virtual machines that are managed by vCenter Server can be in various states of operation and availability. In Horizon Console, you can track the status of machines in the right-hand column of the Machines page.

Table 13-1. Status of Virtual Machines That Are Managed by vCenter Server shows the operational state of virtual-machine desktops that are displayed in Horizon Console. A desktop can be in only one state at a time.

Table 13-1. Status of Virtual Machines That Are Managed by vCenter Server

Status	Description
Provisioning	The virtual machine is being provisioned.
Customizing	The virtual machine in an automated pool is being customized.
Deleting	The virtual machine is marked for deletion. VMware Horizon 8 will delete the virtual machine soon.
Waiting for Agent	Horizon Connection Server is waiting to establish communication with Horizon Agent on a virtual machine in a manual pool.
Maintenance mode	The virtual machine is in maintenance mode. Users cannot log in or use the virtual machine.
Startup	Horizon Agent has started on the virtual machine, but other required services such as the display protocol are still starting. For example, Horizon Agent cannot establish an RDP connection with client computers until RDP has finished starting. The agent startup period allows other processes such as protocol services to start up as well.
Agent disabled	This state can occur in two cases. First, in a desktop pool with the **Delete or refresh machine on logoff** or **Delete machine after logoff** setting enabled, a desktop session is logged out, but the virtual machine is not yet refreshed or deleted. Second, Horizon Connection Server deactivates Horizon Agent just before sending a request to power off the virtual machine. This state ensures that a new desktop session cannot be started on the virtual machine.
Agent unreachable	Horizon Connection Server cannot establish communication with Horizon Agent on a virtual machine.
Invalid IP	The subnet mask registry setting is configured on the virtual machine, and no active network adapters have an IP address within the configured range.
Agent needs reboot	An Horizon 8 component was upgraded, and the virtual machine must be restarted to allow Horizon Agent to operate with the upgraded component.

Table 13-1. Status of Virtual Machines That Are Managed by vCenter Server (continued)

Status	Description
Protocol failure	A display protocol did not start before the Horizon Agent startup period expired. **Note** Horizon Console can display machines in a **Protocol failure** state when one protocol failed but other protocols started successfully. For example, the **Protocol failure** state might be displayed when HTML Access failed but PCoIP and RDP are working. In this case, the machines are available and Horizon Client devices can access them through PCoIP or RDP.
Domain failure	The virtual machine encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Already used	In a desktop pool with the **Delete or refresh machine on logoff** or **Delete machine after logoff** setting enabled, there is no session on the virtual machine, but the session was not logged off. This condition might occur if a virtual machine shuts down unexpectedly or the user resets the machine during a session. By default, when a virtual machine is in this state, Horizon 8 prevents any other Horizon Client devices from accessing the desktop.
Configuration error	The display protocol such as RDP or PCoIP is not enabled.
Provisioning error	An error occurred during provisioning.
Error	An unknown error occurred in the virtual machine.
Unassigned user connected	A user other than the assigned user is logged in to a virtual machine in a dedicated pool. For example, this state can occur if an administrator starts vSphere Client, opens a console on the virtual machine, and logs in.
Unassigned user disconnected	A user other than the assigned user is logged in and disconnected from a virtual machine in a dedicated-assignment pool.
Unknown	The virtual machine is in an unknown state.
Provisioned	The virtual machine is powered off or suspended.
Available	The virtual machine is powered on and ready for a connection. In a dedicated pool, the virtual machine is assigned to a user and will start when the user logs in.
Connected	The virtual machine is in a session and has a remote connection to the Horizon Client device.
Disconnected	The virtual machine is in a session, but it is disconnected from the Horizon Client device.
In progress	The virtual machine is in a transitional state during a maintenance operation.

While a machine is in a particular state, it can be subject to further conditions. Horizon Console displays these conditions as suffixes to the machine state. For example, Horizon Console might display the `Customizing (missing)` state.

Table 13-2. Machine Status Conditions shows these additional conditions.

Table 13-2. Machine Status Conditions

Condition	Description
Missing	The virtual machine is missing in vCenter Server. Typically, the virtual machine was deleted in vCenter Server, but the Horizon LDAP configuration still has a record of the machine.
Task halted	An instant clone task such as push image or a View Composer operation such as refresh, recompose, or rebalance was stopped. The `Task halted` condition applies to all virtual machines that were selected for the operation, but on which the operation has not yet started. Virtual machines in the pool that are not selected for the operation are not placed in the `Task halted` condition.

A machine state can be subject to both conditions, `(missing, task halted)`, if a View Composer task was stopped and the virtual machine is missing in vCenter Server.

Recover Instant-Clone Desktops

When an instant-clone desktop is in an error state, you have the option to recover it. The desktop is recreated from the current base image.

Procedure

1 In Horizon Console, select **Catalog > Desktop Pools**, double-click a pool's ID, and click the **Inventory** tab.

2 Select one or more machines and click **Recover**.

Status of Unmanaged Machines

Unmanaged machines, which are virtual machines not managed by vCenter Server, can be in various states of operation and availability. In Horizon Console, you can track the status of unmanaged machines in the right-hand column of the Machines page under the **Others** tab.

Table 13-3. Status of Unmanaged Machines shows the operational state of unmanaged machines that are displayed in Horizon Console. A machine can be in only one state at a time.

Table 13-3. Status of Unmanaged Machines

Status	Description
Startup	Horizon Agent has started on the machine, but other required services such as the display protocol are still starting. The agent startup period allows other processes such as protocol services to start up as well.
Validating	This state occurs after Horizon Connection Server first becomes aware of the machine, typically after Horizon Connection Server is started or restarted, and before the first successful communication with Horizon Agent on the machine. Typically, this state is transient. It is not the same as the "Agent unreachable" state, which indicates a communication problem.

Table 13-3. Status of Unmanaged Machines (continued)

Status	Description
Agent disabled	This state can occur if Horizon Connection Server deactivates Horizon Agent. This state ensures that a new desktop session cannot be started on the machine.
Agent unreachable	Horizon Connection Server cannot establish communication with Horizon Agent on the machine. The machine might be powered off.
Invalid IP	The subnet mask registry setting is configured on the machine, and no active network adapters have an IP address within the configured range.
Agent needs reboot	A Horizon 8 component was upgraded, and the machine must be restarted to allow Horizon Agent to operate with the upgraded component.
Protocol failure	The display protocol did not start before the Horizon Agent startup period expired. **Note** Horizon Console can display machines in a **Protocol failure** state when one protocol failed but other protocols started successfully. For example, the **Protocol failure** state might be displayed when HTML Access failed but PCoIP and RDP are working. In this case, the machines are available and Horizon Client devices can access them through PCoIP or RDP.
Domain failure	The machine encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Configuration error	The display protocol such as RDP or another protocol is not enabled.
Unassigned user connected	A user other than the assigned user is logged in to a machine in a dedicated-assignment pool. For example, this state can occur if an administrator logs in to the unmanaged machine without using Horizon Client.
Unassigned user disconnected	A user other than the assigned user is logged in and disconnected from a machine in a dedicated-assignment pool.
Unknown	The machine is in an unknown state.
Available	The desktop-source computer is powered on and the desktop is ready for a connection. In a dedicated pool, the desktop is assigned to a user. The desktop starts when the user logs in.
Connected	The desktop is in a session and has a remote connection to a Horizon Client device.
Disconnected	The desktop is in a session, but it is disconnected from the Horizon Client device.

Troubleshooting Machines and Desktop Pools 14

You can use a variety of procedures to diagnose and fix problems that you encounter when you create and use machines and desktop pools.

Users might experience difficulty when they use Horizon Client to access desktops and applications. You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can get assistance from VMware Technical Support.

Read the following topics next:

Display Problem Machines in Horizon Console

You can display a list of the machines whose operation VMware Horizon 8 has detected as being suspect.

Horizon Console displays machines that exhibit the following problems:

- Are powered on, but which are not responding.
- Remain in the provisioning state for a long time.
- Are ready, but which report that they are not accepting connections.
- Appear to be missing from a vCenter Server.

- Have active logins on the console, logins by users who are not entitled, or logins not made from a Connection Server instance.

Procedure

1 In Horizon Console, select **Inventory > Machines**.

2 On the **vCenter** tab, click **Problem Machines** from the Machines drop-down menu.

What to do next

The action that you should take depends on the problem that Horizon Console reports for a machine.

- If a machine is powered on, but does not respond, restart its virtual machine. If the machine still does not respond, verify that the version of the Horizon Agent is supported for the machine operating system. You can use the `vdmadmin` command with the `-A` option to display the Horizon Agent version. For more information, see the *Horizon 8 Administration* document.
- If a machine remains in the provisioning state for a long time, delete its virtual machine, and clone it again. Verify that there is sufficient disk space to provision the machine.
- If a machine reports that it is ready, but does not accept connections, check the firewall configuration to make sure that the display protocol is not blocked.
- If a machine appears to be missing from a vCenter Server, verify whether its virtual machine is configured on the expected vCenter Server, or if it has been moved to another vCenter Server.
- If a machine has an active login, but this is not on the console, the session must be remote. If you cannot contact the logged-in users, you might need to restart the virtual machine to forcibly log out the users.

Verify User Assignment for Desktop Pools

For dedicated user assignments, you can verify if the user that is assigned to the virtual machine is the user that connects to the virtual desktop or not.

Prerequisites

- Verify that the virtual machine belongs to a dedicated-assignment pool. In Horizon Console, the desktop pool assignment appears in the **User Assignment** column on the **Desktop Pools** page.
- Verify that you have entitled users to the desktop pool.

Procedure

1 In Horizon Console, select **Inventory > Machines**.

2 On the **vCenter** tab, choose to view the assigned user or connected user.

Option	Description
Assigned User	The **Assigned User** column displays the user who is assigned to the desktop pool. **Note** The **Assigned User** column does not display any user for a floating desktop pool.
Connected User	The **Connected User** column displays the user who is connected to the virtual machine. Most of the time, the **Connected User** is the same as the **Assigned User** when the assigned user is connected to the desktop. At other times, when an administrator is connected to the virtual machine, the **Connected User** column displays the administrator.

Restart Desktops and Reset Virtual Machines in Horizon Console

You can perform a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine. You can perform a reset operation on a virtual machine without the graceful operating system restart, which performs a hard power-off and power-on of the virtual machine.

VMs maintain their network assignment when a restart or reset operation is performed.

State	Description
In Progress	VM is working in state transformation, e.g., restarting.
Provisioned	When a VM is fully provisioned, it is shut down or powered off and waiting to begin boot process.
Agent Unreachable	VM is loaded, but the agent is not responding. Either boot still in progress or shutting down or lost network connection.
Available	Agent is available.

Table 14-1. Reset and Restart Functionality

Pool Type	Reset Functionality (Pools, Machines, Sessions, and Horizon Clients)	Restart Functionality (Pools, Machines, Sessions, and Horizon Clients)
Full-clone pool (dedicated pool and floating pool without delete on logOff option enabled)	Reset the VM (Power Off and Power On VM)	Restart the VM (Graceful OS restart)
Instant-clone pool (floating pool)	**Power Off VM > Delete VM > Create new VM > Power On**	**Graceful OS shut down > Delete VM > Create new VM > Power On**
Published desktop pools	NA (Not Supported)	NA (Not Supported)

Procedure

1 In Horizon Console, select **Inventory > Machines**.

2 On the **vCenter** tab, choose to restart a virtual desktop or reset a virtual machine.

Option	Description
Restart Desktop	Restarts the virtual machine with a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.
Reset Virtual Machine	Resets the virtual machine without a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.

3 Click **OK**.

Send Messages to Desktop Users in Horizon Console

You might sometimes need to send messages to users who are currently logged into desktops. For example, if you need to perform maintenance on machine, you can ask the users to log out temporarily, or warn them of a future interruption of service. You can send a message to multiple users (there is no set limit on the number of users).

Procedure

1 In Horizon Console, click **Inventory > Desktops**.

2 Click a pool ID and click the **Sessions** tab.

3 Select one or more machines and click **Send Message**.

4 Type the message, select the message type, and click **OK**.

A message type can be **Info**, **Warning**, or **Error**.

Results

The message is sent to all selected machines in active sessions.

Manage Machines and Policies for Unentitled Users in Horizon Console

You can display the machines that are allocated to users whose entitlement has been removed, and you can also display the policies that have been applied to unentitled users.

A user who is unentitled might have left the organization permanently, or you might have suspended their account for an extended period of time. These users are assigned a machine but they are no longer entitled to use the machine pool.

You can also use the `vdmadmin` command with the `-O` or `-P` option to display unentitled machines and policies. For more information, see the *Horizon 8 Administration* document.

Procedure

1 In Horizon Console, select **Inventory > Machines**.

2. Select **More Commands > View Unentitled Machines**.
3. Remove the machine assignments for unentitled users.
4. Select **More Commands > View Unentitled Machines** or **More Commands > View Unentitled Policies** as appropriate.
5. Change or remove the policies that are applied to unentitled users.

Collect Diagnostic Information for a Linux Virtual Machine

You can collect diagnostic information to help VMware Technical Support diagnose and resolve issues with a Linux virtual machine that you are using to provision remote Horizon 8 resources. You create a Data Collection Tool (DCT) bundle that gathers the machine's configuration information and logs into a compressed tarball.

For more information, see "Using DCT to Collect Logs for Remote Desktop Features and Components" in the *Horizon 8 Administration* document.

Procedure

1. Log in to the Linux virtual machine as a user with the required privileges.
2. Open a command prompt and run the `dct-debug.sh` script.

   ```
   sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
   ```

Results

The script generates a tarball that contains the DCT bundle. For example:

```
ubuntu-18-vdm-sdct-20190201-0606-agent.tgz
```

The tarball is generated in the directory from which the script was executed (the current working directory).

Troubleshooting Instant Clones in the Internal VM Debug Mode

You can use the internal VM debug mode to troubleshoot internal virtual machines in instant-clone desktop pools and instant-clone farms. With the internal VM debug mode, you can analyze failed internal virtual machines before these virtual machines are deleted. You must enable the internal VM debug mode before you create an instant-clone desktop pool or farm.

Procedure

1. In vSphere Client, select the golden-image VM, and click **Manage > Configure > VM Options > Edit > VM Options > Advanced > Edit Configuration**.

   The **Configuration Parameters** window displays a list of parameter names and values.

2 In the **Configuration Parameters** window, search for the `cloneprep.debug.mode` parameter.

   If the golden-image VM does not have the `cloneprep.debug.mode` parameter, you must add `cloneprep.debug.mode` as the parameter name and add a value of ON or OFF. If the golden VM has the `cloneprep.debug.mode` parameter, you can change the value of the parameter to ON or OFF.

3 Enable or deactivate the internal VM debug mode for internal VMs.

   - To enable the internal VM debug mode, set the value of `cloneprep.debug.mode` to ON. If you enable the internal VM debug mode, the internal VMs are not locked and cannot be deleted by Horizon Connection Server.
   - To deactivate the internal VM debug mode, set the value of `cloneprep.debug.mode` to OFF. If you deactivate the internal VM debug mode, the internal VMs are locked and can be deleted by Horizon Connection Server.

   For instant-clone actions such as prime, provision, resync, or unprime, the internal virtual machines use the value set in the golden virtual machine. If you do not deactivate the internal VM debug mode, then the VMs remain in vCenter Server till you delete the VMs. For further debugging on instant clone actions, you can also log in to the internal VM and view the instant clone logs. You can also see the following VMware Knowledge Base articles for further debugging of instant-clone actions:

   - Initial publish of an Instant Clone desktop pool image fails and the template VMs are deleted (2144938) https://kb.vmware.com/s/article/2144938
   - How to change SVGA settings for Instant Clone Pools (2151745) https://kb.vmware.com/s/article/2151745

Horizon Agent Fails to Disconnect on an iPad Pro Horizon Client

The Horizon Agent connection on a SLED/SLES machine fails to disconnect after a restart or shutdown on a iPad Pro Horizon Client.

Problem

When you restart or shutdown a SLED/SLES virtual machine on an iPad Pro Horizon Client, the desktop does not respond. Horizon Agent fails to disconnect.

Cause

The SLED/SLES machine might not be sending messages correctly to Horizon Client after a restart or shutdown operation.

Solution

◆ Disconnect the desktop connection manually from iPad Pro Horizon Client.

SSO Fails to Connect to a PowerOff Agent

Single Sign-On (SSO) does not connect to a PowerOff agent.

Problem

When you log in as a broker and connect to an agent, SSO fails to connect to the PowerOff agent.

Solution

- Manually log in to the desktop, or disconnect and reconnect to the agent again.

Unreachable VM After Creating a Manual Desktop Pool for Linux

The virtual machine state is not responding.

Problem

The virtual machine status might be Waiting for Agent or Unreachable after you create a Manual Desktop Pool.

Cause

There might be several user error configuration or setup causes for the virtual machine state to be Unreachable or Waiting for Agent.

- Verify that the option `machine.id` exists in the virtual machines vmx configuration file.

  If it does not exist, then verify that the virtual machine was added to the desktop pool correctly. Else recreate the desktop pool to let the broker rewrite the option to the vmx configuration file.
- Verify that the VMware Tool or Open VM Tool is installed correctly.

  If the steps to install VMware Tool or Open VM Tool were not performed correctly, the `vmware-rpctool` command might not exist under `PATH` in the Linux virtual machine. You must follow the guide to install VMware Tool or Open VM Tool.

  Run the command after you finish installing.

  ```
  #vmware-rpctool "machine.id.get"
  ```

  The machine.id values are listed from the virtual machines vmx configuration file.
- Verify if the FQDN of the broker can be resolved to the IP Address in the agent Linux virtual machine.

Setting Up Published Desktops and Applications in Horizon

15

This section describes how to create and deploy pools of desktops and applications that run on Microsoft Remote Desktop Services (RDS) hosts.

It includes information about configuring policies, entitling users and groups, and configuring remote application features.

Read the following topics next:

Introduction to Multi-session Published Desktops and Applications

With VMware Horizon 8, you can create published desktops associated with a farm of multi-session hosts. You can also deliver a published application to many users by creating application pools. The published applications in application pools run on a farm of multi-session hosts.

A Windows-based farm consists of a group of Windows Remote Desktop Services (RDS) hosts. With the addition of App Volumes, you can have Windows applications delivered dynamically using published applications on demand to help reduce the number of OS images and RDS farms.

A Linux-based farm consists of a group of multi-session host machines running a supported Linux distribution, as described in Considerations for Linux Farms, Published Desktops, and Published Applications.

Farms, Multi-session Hosts, and Published Desktops and Applications

With Windows-based farms, you can use Microsoft Remote Desktop Services (RDS) to provide published desktops on RDS hosts and deliver published applications to many users. You can also provide published desktops and applications from a farm of Linux-based multi-session hosts.

Multi-session Host

The following types of machines can serve as multi-session hosts.

- Windows-based server computers that have Windows Remote Desktop Services (RDS) and Horizon Agent installed. These servers host applications that users can access remotely.
- Linux-based machines running a Linux distribution that supports multi-session capabilities, as described in Considerations for Linux Farms, Published Desktops, and Published Applications.

Farms

A farm is a collection of multi-session hosts. Farms facilitate the management of hosts, along with the published desktops and applications provisioned from those hosts, across an enterprise. Farms provide a common set of published applications or published desktops to serve groups of users that vary in size or have different desktop or application requirements.

When you create a published desktop or application pool, you must specify one and only one farm. The hosts in a farm can host published desktops, applications, or both. A farm can support at most one published desktop pool, but it can support multiple application pools. A farm can support desktop pools and application pools simultaneously.

Farms can have a variable number of multi-session hosts. See VMware Configuration Maximums for the maximum number of host machines supported per farm. VMware Horizon 8 provides load balancing of the hosts in a farm by directing connection requests to the host that has the least number of active sessions.

Published Desktop Pool

A published desktop pool is provisioned from a farm of multi-session host machines. Each published desktop can support multiple user sessions at a time.

Published desktops require fewer virtual machine resources than single-session virtual desktops. A published desktop is based on a session to a multi-session host. In contrast, a desktop in an single-session desktop pool is based on a virtual machine.

Published Application Pool

A published application pool runs on a farm of multi-session host machines.

With a published application pool, you can deliver a single application to many users simultaneously. When you create a published application pool, you deploy an application in the data center that users can access from anywhere on the network.

Published Applications on Demand

Published applications on demand are attached to an available Windows RDS host only at the time a user launches an application. Additionally, users' applications are activated only within their session. By removing the need to plan for grouping applications to farms, this model minimizes the number of hosts required to support your users and their applications as well as associated infrastructure costs and management time.

Configure VMware Horizon 8 for Published Desktops Delivery

You can enable Horizon 8 to deliver published desktops on existing or new multi-session hosts.

Procedure

1. To configure Horizon 8 to deliver published desktops on existing multi-session hosts, complete the following tasks:

   a. Prepare existing multi-session hosts for Horizon 8.

      - Windows RDS hosts can be physical or virtual machines. See Setting Up Remote Desktop Services Hosts.

      - To configure a Linux-based multi-session host, follow the steps described in Creating and Preparing a Linux Virtual Machine for Cloning. Ensure that you install Horizon Agent with the `--multiple-session` parameter included.

   b. Create a manual farm. A manual farm consists of multi-session hosts that already exist. You manually add the hosts when you create the farm. See Create a Manual Farm in Horizon.

   c. Create a published desktop pool for the manual farm you created. See Create a Published Desktop Pool.

   d. Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon 8 Administration* document.

2. To configure Horizon 8 to deliver published desktops on new multi-session hosts, complete the following tasks:

   a. Prepare an RDS host golden image virtual machine. Horizon 8 clones the RDS hosts from this machine as part of the farm creation process. See Prepare an RDS Host Golden Image Virtual Machine.

   b. Create an automated farm. An automated farm consists of RDS hosts that Horizon create as instant-clone virtual machines in vCenter Server. See Create an Automated Instant-Clone Farm in Horizon.

   c. Create a published desktop pool for the automated farm you created. See Create a Published Desktop Pool.

   d. Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon 8 Administration* document.

Configure Horizon 8 for Published Applications Delivery

You can enable Horizon 8 to deliver published applications on existing or new RDS hosts.

Procedure

1 To configure Horizon 8 to deliver published applications on existing RDS hosts, complete the following tasks:

   a Prepare existing RDS hosts for Horizon 8. The RDS hosts can be physical or virtual machines. See Setting Up Remote Desktop Services Hosts

   b Create a manual farm. A manual farm consists of RDS hosts that already exist. You manually add the RDS hosts when you create the farm. See Create a Manual Farm in Horizon.

   c Create a published application pool for the manual farm you created. See Create an Application Pool.

   d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon 8 Administration* document.

2 To configure Horizon 8 to deliver published applications on new RDS hosts, complete the following tasks:

   a Prepare an RDS host golden image virtual machine. Horizon 8 clones the RDS hosts from this machine as part of the farm creation process. See Prepare an RDS Host Golden Image Virtual Machine.

   b Create an automated farm. An automated farm consists of RDS hosts that Horizon create as instant-clone virtual machines in vCenter Server. See Create an Automated Instant-Clone Farm in Horizon.

   c Create a published application pool for the automated farm you created. See Create an Application Pool.

   d Entitle users and groups. See, "Entitling Users and Groups" in the *Horizon 8 Administration* document.

Configure Horizon 8 for Published Applications on Demand Delivery

You can enable Horizon 8 to deliver published applications on demand to an automated RDS farm.

To access published applications on demand, you add one or more VMware App Volumes Managers to Horizon Console, associate it with a farm, select applications and add user and group entitlement. These tasks need to be performed in the order in which they are documented.

Prerequisites

Ensure that your environment includes the minimum product versions for this feature listed below:

- Horizon Agent 2212
- VMware App Volumes 4, version 2212

Procedure

1 Add the App Volumes Manager from where you want to access applications. See Add a VMware App Volumes Manager in the *Horizon 8 Installation and Upgrade* document.

  The App Volumes Manager must be configured with an SSL certificate signed by a trusted CA. For a self-signed certificate, import the App Volumes Manager certificate to a trusted root store.

2 Import one or more application package to the App Volumes Manager.

3 Prepare an RDS host golden image virtual machine. Horizon 8 clones the RDS hosts from this machine as part of the farm creation process. For more information, see Prepare an RDS Host Golden Image Virtual Machine.

  Note RDS farms should be created using a golden image that has Windows Update disabled. Windows Updates should be applied by updating the golden image and scheduling maintenance for the farm to apply the new golden image.

4 Create an automated farm. An automated farm contains the RDS hosts that Horizon 8 creates as instant-clone virtual machines in vCenter Server.For more information, see Create an Automated Instant-Clone Farm in Horizon.

5 Associate the App Volumes Manager with a farm. For more information, see Associate App Volumes Manager with a Farm.

6 Create a published application pool. For more information, see Create an Application Pool.

7 Entitle users and groups. For more information, see Entitling Users and Groups in the *Horizon 8 Administration* document

Considerations for Linux Farms, Published Desktops, and Published Applications

Keep in mind the following feature limitations and considerations when working with Linux farms, published desktop pools, and published application pools.

- Only virtual machines running RHEL Workstation 7.9/8.x/9.x, Rocky Linux 8.x/9.x, Ubuntu 20.04/22.04, or Debian 10.x/11.x/12.x can support multi-session published desktop pools and single-session or multi-session application pools.

- Published applications support vGPU capabilities with the following restrictions.
  - You must deploy the Horizon 8 components in a VMware virtualized environment running vSphere 7 U3 or later.
  - When using vSphere Client to configure vGPU settings for the Linux desktop VM, you must select the profile that assigns the full memory of the physical GPU to the VM. This means selecting the highest available vGPU profile from the list of options. See Configure a Shared PCI Device for vGPU on the Linux VM .
- Published desktops and applications are not supported on the KDE desktop environment.
- All the host machines in a farm must be running the same operating system. For example, you can create a farm consisting of all Linux hosts or Windows hosts, but you cannot create a farm consisting of a mix of Linux and Windows hosts.
- All the Linux host machines in a farm must be running the same Linux distribution. For example, you can create a farm containing all RHEL Workstation 9.0 hosts or all Ubuntu 22.04 hosts, but you cannot create a farm containing a mix of RHEL Workstation 9.0 and Ubuntu 22.04 hosts.
- Published desktops do not support the following features:
  - USB redirection
  - Smart card redirection
- True SSO is supported on multi-session published desktops and applications based on the following types of farms.
  - Manual and automated instant-clone farms of Ubuntu 20.04/22.04, Debian 10.x, or RHEL Workstation 7.9 host machines that have been integrated with Active Directory using the Samba domain-join method.
  - Manual and automated instant-clone farms of RHEL Workstation 8.x/9.x, Rocky Linux 8.x/9.x, or Debian 11.x/12.x host machines that have been integrated with Active Directory using the System Security Services Daemon (SSSD) domain-join method.
- Each published desktop or published application can support up to 50 user sessions, if the host Linux virtual machine meets the minimum vCPU and vMemory requirements. For more information, see Create a Virtual Machine and Install Linux.
- To make it faster for users to start a remote session, Horizon Agent can pre-launch a specified number of sessions per host machine. You can specify the number of pre-launched sessions by using the **MaxSessionsBuffer** configuration option in `/etc/vmware/viewagent-custom.conf`. See Edit Configuration Files on a Linux Desktop.
- When running a Linux published application from Horizon Client for Windows, users can improve the application performance by setting the preference to hide window contents while dragging. For example, navigate to **Control Panel > System and Security > System > Advanced system settings > Advanced > Settings** and deselect **Show window contents while dragging**.

- When logging in to a desktop to connect to a published application, users must enable **Classic (X11 display server)**. Otherwise, the application window is displayed incorrectly, such as without minimize and maximize buttons.
- When connecting to a Linux published application from a client system using a multiple-monitor configuration, verify that all monitors have the identical scale setting. Otherwise, the application window cannot be moved between monitor screens.
- Linux published applications do not support enabling the **Multi-Session Mode** setting in the configuration wizard for application pools. When you create a Linux application pool, you can only configure it in single-session mode. For example, if a user opens a published application on client A and then opens the same published application or another published application based on the same farm on client B, then the session on client A is disconnected and reconnected on client B.
- Horizon Agent for Linux does not support session stealing between published desktops and published applications.

  For example, if a user has opened a published desktop session and then attempts to open an application session based on the same farm, the desktop session remains active and the application session is not established. Likewise, if the user has opened an application session and then attempts to open a published desktop session based on the same farm, the application session remains active and the desktop session is not established.

Setting Up Remote Desktop Services Hosts

Microsoft Remote Desktop Services (RDS) hosts provide desktop sessions and applications that users can access from client devices. If you plan to create published desktop pools or application pools, you must first set up RDS hosts.

Remote Desktop Services Hosts

An RDS host is a server computer that hosts applications and desktop sessions for remote access. An RDS host can be a virtual machine or a physical server.

An RDS host has the Microsoft Remote Desktop Services role, the Microsoft Remote Desktop Session Host service, and Horizon Agent installed. Remote Desktop Services was previously known as Terminal Services. The Remote Desktop Session Host service allows a server to host applications and remote desktop sessions. With Horizon Agent installed on an RDS host, users can connect to applications and desktop sessions by using the display protocol PCoIP or Blast Extreme. Both protocols provide an optimized user experience for the delivery of remote content, including images, audio and video.

To set up an RDS host, you must complete the following tasks:

1 Prepare Windows Server operating systems for RDS host use. See Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use.

2 Install Remote Desktop Services on Windows Server operating systems. See Install Remote Desktop Services on Windows Server 2016, 2019, or 2022.

3 Install desktop experience on Windows Server operating systems. See Install Desktop Experience on Windows Server 2016 or 2019.

4 Restrict users to a single session. See Restrict Users to a Single Session.

5 Install Horizon Agent on an RDS host. See Install Horizon Agent on a Remote Desktop Services Host .

6 Install App Volumes agent on the RDS host if you plan to deliver published applications on demand. See the *Install App Volumes Agent* section in the *VMware App Volumes Installation Guide*.

Note If smart card authentication is enabled, make sure that the Smart Card service is disabled on RDS hosts. Otherwise, authentication might fail. By default, this service is disabled.

Caution When a user launches an application, for example, a Web browser, it is possible for a user to gain access to the local drives on the RDS host that is hosting the application. This can happen if the application provides functions that cause Windows Explorer to run. Do not create published desktop pools and application pools on the same farm so that desktop sessions are not affected.

Installing Applications

If you plan to create application pools, you must install the applications on the RDS hosts. If you want Horizon 8 to automatically display the list of installed applications, you must install the applications so that they are available to all users from the **Start** menu. You can install an application at any time before you create the application pool. If you plan to manually specify an application, you can install the application at any time, either before or after creating an application pool.

Important When you install an application, you must install it on all the RDS hosts in a farm and in the same location on each RDS host. If you do not, a health warning will appear on the Horizon Console dashboard. In such a situation, if you create an application pool, users might encounter an error when they try to run the application.

When you create an application pool, Horizon 8 automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all of the RDS hosts in a farm. You can choose any applications from that list. In addition, you can manually specify an application that is not available to all users from the **Start** menu. There is no limit on the number of applications that you can install on an RDS host.

You can use a combination of applications installed on RDS hosts and applications on demand. For applications on demand, applications need not be installed on RDS hosts.

Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use

To use a Windows Server 2016, Windows Server 2019, or Windows Server 2022 machine as an RDS host, you must perform certain steps before you install Horizon Agent in the virtual machine.

When the Remote Desktop Session Host (RDSH) role is not present, the Horizon Agent installer prompts you to install Horizon Agent in RDS mode or desktop mode. If RDS mode is selected, the installer will install the RDSH role as well as the Desktop Experience role for the supported operating systems and prompt you to reboot the system. At this time the installer has not yet installed Horizon Agent. After rebooting the system you must run the installer again to continue installing Horizon Agent in RDS mode.

When the Remote Desktop Session Host role is present, the Horizon Agent installer does not display these options. The installer treats the Windows Server machine as an RDS host instead of a single-session Horizon desktop and installs Horizon Agent in RDS mode. During this installation, the Horizon Agent installer will not automatically install the Desktop Experience role. If you need the Desktop Experience role, you must install the role manually. See Install Desktop Experience on Windows Server 2016 or 2019.

Note The Desktop Experience Role is required for the following features:

- HTML Access
- Scanner redirection
- Windows Aero

The Desktop Experience option is available only during the OS installation, so the Horizon Agent installer installs the RDSH role on Windows Server 2016 and later.

Prerequisites

- Verify that the RDS host is part of the Active Directory domain for the Horizon 8 deployment.
- Familiarize yourself with the steps to install the Desktop Experience feature on supported Windows Server operating systems. See Install Remote Desktop Services on Windows Server 2016, 2019, or 2022.
- On Windows Server 2016 machines, familiarize yourself with the steps to configure the Windows Firewall service to restart after failures occur.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.

Procedure

1 Log in as an administrator.

2 To start the Horizon Agent installation program, double-click the installer file.

   The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

3 Accept the VMware license terms.

4 Select **RDS mode** to install the RDSH role and/or the Desktop Experience role. After it is installed, the installer will prompt you to restart the system. After the system is restarted, launch the installer again to continue installing Horizon Agent in RDS mode.

5 On Windows Server 2016 machines, configure the Windows Firewall service to restart after failures occur.

What to do next

Install Horizon Agent on the remote desktop services host. See Install Horizon Agent on a Remote Desktop Services Host .

Install Remote Desktop Services on Windows Server 2016, 2019, or 2022

Remote Desktop Services is one of the roles that a Windows Server 2016, 2019 or 2022 can have. You must install this role to set up an RDS host.

To use a Windows Server machine as an RDS host, see Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use.

Prerequisites

- Verify that the RDS host is running a supported Windows Server version.
- Verify that the RDS host is part of the Active Directory domain for the Horizon 8 deployment.

Procedure

1 Log in to the RDS host as an administrator.

2 Start Server Manager.

3 Select **Add roles and features**.

4 On the Select Installation Type page, select **Role-based or feature-based installation**.

5 On the Select Destination Server page, select a server.

6 On the Select Server Roles page, select **Remote Desktop Services**.

7 On the Select Features page, accept the defaults.

8 On the Remote Desktop Services, Role Services page, select the **Remote Desktop Session Host** role and accept the prompts to add in the additional features required to support the Desktop Session Host role.

9 Follow the prompts to finish the installation.

10 Restart the Windows server.

What to do next

If you plan to use HTML Access or scanner redirection, install the Desktop Experience feature.

Restrict users to a single desktop session. See Restrict Users to a Single Session.

Install Desktop Experience on Windows Server 2016 or 2019

For published desktops and applications, and for virtual desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Note A Windows Server 2016 and Windows Server 2019 installation with the Desktop Experience option installs the standard user interface and all tools, including the client experience and the desktop experience features. For Windows Server 2016 or Windows Server 2019 installation, select **Windows Server 2016** or **Windows Server 2019** or **Windows Server (Server with Desktop Experience)**. If you do not make a choice in the Setup wizard, Windows Server 2016 or Windows Server 2019 is installed as the Server Core installation option. You cannot switch between the installation options. If you install **Windows Server (Server with Desktop Experience)**, and later decide to use **Windows Server 2016** or **Windows Server 2019**, you must perform a fresh installation of Windows Server 2016 or Windows Server 2019.

Procedure

1 Log in as an administrator.

2 Start Server Manager.

3 Select **Add roles and features**.

4 On the Select Installation Type page, select **Role-based or feature-based installation**.

5 On the Select Destination Server page, select a server.

6 On the Select Server Roles page, accept the default selection and click **Next**.

7 On the Select Features page, under **User Interfaces and Infrastructure**, select **Desktop Experience**.

8 Follow the prompts and finish the installation.

Restrict Users to a Single Session

You must configure the RDS host to restrict users to a single sessions using a group policy setting.

Procedure

1. In the folder `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections`, Click **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**.
2. Enable the group policy setting `Restrict Remote Desktop Services users to a single Remote Desktop Services session`.

What to do next

Install Horizon 8 Agent on the RDS host. See Install Horizon Agent on a Remote Desktop Services Host.

Caution When a user launches an application, for example, a Web browser, it is possible for a user to gain access to the local drives on the RDS host that is hosting the application. This can happen if the application provides functions that cause Windows Explorer to run. Do not create published desktop pools and application pools on the same farm so that desktop sessions are not affected.

Install Horizon Agent on a Remote Desktop Services Host

Horizon Agent communicates with Connection Server and supports the display protocols PCoIP and Blast Extreme. You must install Horizon Agent on an RDS Host.

Prerequisites

- Verify that you have prepared Active Directory. See the *Horizon 8 Installation and Upgrade* document.
- To use a Windows Server virtual machine as an RDS host, see Prepare Windows Server Operating Systems for Remote Desktop Services (RDS) Host Use.
- Install the Remote Desktop Services role described in Install Remote Desktop Services on Windows Server 2016, 2019, or 2022.
- Restrict users to a single desktop session. See Restrict Users to a Single Session.
- Familiarize yourself with the Horizon Agent custom setup options. See Horizon Agent Custom Setup Options for an RDS Host.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.

Procedure

1. Log in as an administrator.

2 To start the Horizon Agent installation program, double-click the installer file.

   The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number and *xxxxxx* is the build number.

3 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

   You must install all Horizon 8 components with the same IP version.

4 Select your custom setup options.

5 In the **Server** text box, type the host name or IP address of a Connection Server host.

   Horizon Agent installer prompts this step only if you are installing Horizon Agent on an RDS host that will be in a manual farm. During installation, the installer registers the RDS host with this Connection Server instance. After registration, the specified Connection Server instance and any additional instances in the same Connection Server group can communicate with the RDS host.

6 Select an authentication method to register the RDS host with the Connection Server instance.

Option	Description
Authenticate as the currently logged in user	The **Username** and **Password** text boxes are disabled and you are logged in to the Connection Server instance with your current username and password.
Specify administrator credentials	You must provide the username and password of a Connection Server administrator in the **Username** and **Password** text boxes.

   The user account must be a domain user with access to View LDAP on the Connection Server instance. A local user does not work.

7 Follow the prompts and finish the installation.

What to do next

Create a farm. See Creating and Managing Farms.

Horizon Agent Custom Setup Options for an RDS Host

When you install Horizon Agent on an RDS host, you can select custom setup options. In addition, Horizon Agent installs certain features automatically on all guest operating systems on which they are supported. These features are not optional.

To change custom setup options after you install the latest Horizon Agent version, see Modify Installed Components with theHorizon Agent for Windows Installer.

Table 15-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 or IPv6 Environment

Option	Description
USB Redirection	Gives users access to locally connected USB storage devices. This setup option is not selected by default. You must select the option to install it. For information about using USB redirection securely, see the *Horizon Security* document. For example, you can use group policy settings to disable USB redirection for specific users. For information about using the USB redirection feature, and USB device type limitations, see "Using USB Devices with Remote Desktops and Applications" in the *Horizon Remote Desktop Features and GPOs* document.
HTML Access	Enables users to connect to published desktops and published applications by using HTML Access. The HTML Access Agent is installed when this setup option is selected. This agent must be installed on RDS hosts to enable users to make connections with HTML Access
3D RDSH	Provides 3D graphics support to applications that run on this RDS host.
Client Drive Redirection	Enables Horizon Client users to share local drives with their published desktops and published applications. After this setup option is installed, no further configuration is required on the RDS host.
Help Desk Plugin for Horizon Agent	You must have a Horizon Enterprise edition license or Horizon Apps Advanced edition license for Horizon to use the Help Desk Tool. This option is installed and enabled by default.
Horizon Monitoring Service Agent	Enables Horizon Monitoring Agent, which is used to provide metrics to Cloud Monitoring Service (CMS).
Scanner Redirection	Redirects scanning devices that are connected to the client system so that they can be used on the published desktop or published application. You must install the Desktop Experience feature in the Windows Server operating system on the RDS hosts to make this option available in the Horizon Agent installer. This setup option is not installed by default on Windows Server guest operating systems. You must select the option to install it.
Serial Port Redirection	Redirects serial COM ports that are connected to the client system so that they can be used on the published desktop or published application. This option is not selected by default. You must select the option to install it.
Instant Clone	Enables the creation of instant-clone virtual machines on a farm of RDS hosts. This setup option is not installed by default on Windows Server guest operating systems. You must select the option to install it.
Horizon Performance Tracker	Monitors the performance of the display protocol and system resource usage. This option is not selected by default. You must select the option to install it. .NET Framework 4.0 or later is required if you install Horizon Performance Tracker.
VMware Integrated Printing	Enables users to print to any printer available on their client machines. Location-based printing is supported. VMware Integrated Printing is supported on the following remote desktops and applications: ■ Virtual desktops deployed on Windows Server operating systems or Windows Client operating systems. ■ Published desktops and published applications that are deployed on RDS hosts, where the RDS hosts are virtual machines or physical machines

Table 15-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 or IPv6 Environment (continued)

Option	Description
Hybrid Logon	Provides unauthenticated access users access to network resources without the need to enter credentials. This setup option is not installed by default. You must select the option to install it.
Geolocation Redirection	Enables the Geolocation Redirection feature. This option is not selected by default. You must select the option to install it.

Some remote experience features are installed automatically on an RDS host.

Table 15-2. Horizon Agent Features That Are Installed Automatically on an RDS Host

Feature	Description
PCoIP Agent	Enables users to use the PCoIP display protocol to connect to applications and published desktops.
Windows Media Multimedia Redirection (MMR)	Provides multimedia redirection for published desktops. This feature delivers a multimedia stream directly to the client computer, which enables the multimedia stream to be processed on the client hardware instead of on the remote ESXi host.
Unity Touch	Enables tablet and smart phone users to interact with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications without using the Start menu or Taskbar.
PSG Agent	Installs the PCoIP Secure Gateway on RDS hosts to implement the PCoIP display protocol for desktop and application sessions that run on RDS hosts.
VMwareRDS	Provides the VMware implementation of Remote Desktop Services functionality.
HTML5 Multimedia Redirection	Redirects HTML5 multimedia content in a Chrome or Edge browser to the client for performance optimization.
Browser Redirection	Renders a website on the client system instead of the agent system, and displays the website over the remote browser's viewport, when a user uses the Chrome browser in a remote desktop.

In an IPv6 environment, the automatically installed features are PCoIP Agent, PSG Agent, and VMwareRDS.

For additional features that are supported on RDS hosts, see "Feature Support Matrix for Horizon Agent" in the *Horizon Overview and Deployment Planning* document.

Modify Installed Components with theHorizon Agent for Windows Installer

The Horizon Agent for Windows installer allows you to modify already installed components without needing to uninstall and reinstall Horizon Agent.

You can run the Horizon Agent installer on a virtual machine where Horizon Agent is already installed to modify, repair, or remove previously installed components. You can also change custom setup options silently using the command line.

Note You cannot switch between installation types, such as managed to unmanaged machines. You also cannot modify Instant Clone Agent (NGVC).

Procedure

1 To start the Horizon Agent installation program, double-click the installer file. The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

  You can also use the **Uninstall or change a program** in the Control Panel: Click **VMware Horizon Agent**, then click **Change**.

2 Select **Modify** from these three options:

  - Modify: add or remove the components that are installed.
  - Repair: fix missing or corrupt files, shortcuts, and registry entries.
  - Remove: remove Horizon Agent from the computer.

3 Select or deselect features to add or remove them from the list.

4 Follow the prompts to finish the installation.

5 Restart the system for the changes to take effect.

What to do next

You can confirm the components that were removed (Absent) or added (Local) in the registry located at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\Installer\Features_HorizonAgent`.

Silent Installation Properties for Horizon Agent for Windows

You can include specific properties when you silently install Horizon Agent for Windows from the command line. You must use a *`PROPERTY=value`* format so that Microsoft Windows Installer (MSI) can interpret the properties and values. A silent upgrade uses the same install commands. You can also modify already installed Horizon Agent components silently.

The following table shows the Horizon Agent silent installation properties that you can use at the command-line.

Table 15-3. MSI Properties for Silently Installing Horizon Agent

MSI Property	Description	Default Value
`ENABLE_UNC_REDIRECTION`	Specifies whether the UNC Path Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which UNCs to redirect. See "Configuring UNC Path Redirection" in the *Horizon Remote Desktop Features and GPOs* document. This MSI property is optional.	0
`HORIZON_MONITOR_ENABLED`	Specifies whether to enable or disable Horizon monitoring mode. This flag works only if you have VMware Horizon Cloud Service - next-gen installed in your environment. A value of 1 enables Horizon monitoring mode. A value of 0 disables Horizon monitoring.	0
`IGNORE_DOTNET_CHECK`	Determines whether the installer checks for a minimum .NET version. By default, when Horizon Performance Tracker is selected, the installer performs a pre-check to confirm that .NET 4.6.2 or later is installed, and stops the install process if it is not. A value of 1 cancels this pre-check. A value of 0 allows the pre-check to proceed.	`%ProgramFiles%\VMware\VMware View\Agent`
`INSTALLDIR`	Path and folder in which the Horizon Agent software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	
`RDP_CHOICE`	Determines whether to enable Remote Desktop Protocol (RDP) on the desktop. A value of 1 enables RDP. A value of 0 leaves the RDP setting deactivated. This MSI property is optional.	1
`SUPPRESS_RUNONCE_CHECK`	Ignores pending Windows Update tasks scheduled at the next operating system reboot in the `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` and `RunOnceEx` keys. Using this flag allows concurrent installation but does not guarantee the installation outcome when the system updates affect the Horizon Agent run-time dependencies. This MSI property is optional.	None
`URL_FILTERING_ENABLED`	Specifies whether the URL Content Redirection feature is installed. A value of 1 installs the feature. You must use group policy settings to configure which URLs to redirect. See "Configuring URL Content Redirection" in the *Horizon Remote Desktop Features and GPOs* document. This MSI property is optional.	0
`VDM_SKIP_BROKER_REGISTRATION`	A value of 1 skips unmanaged desktops.	None

Table 15-3. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
VDM_VC_MANAGED_AGENT	Determines whether vCenter Server manages the virtual machine on which Horizon Agent is installed. A value of 1 configures the desktop as a vCenter Server-managed virtual machine. A value of 0 configures the desktop as unmanaged by vCenter Server. This MSI property is required. **Note** The installer repair option is not supported for an unmanaged installation. Repairing such an installation results in an installation of a managed Horizon Agent.	None
VDM_REINSTALL	Specifies a list of already installed features delimited by commas that are to be reinstalled, applicable only in silent mode.	None
VDM_REINSTALLMODE	A string containing letters that specifies the type of reinstall to perform, applicable only in silent mode. See https://learn.microsoft.com/en-us/windows/win32/msi/reinstallmode for details on which options to use.	None
VDM_SERVER_NAME	Host name or IP address of the Connection Server instance on which the Horizon Agent installer registers an unmanaged desktop. This property applies to unmanaged desktops only. For example: `VDM_SERVER_NAME=10.123.01.01` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
VDM_SERVER_USERNAME	User name of the administrator on the Connection Server instance. This MSI property applies only to unmanaged desktops. For example: `VDM_SERVER_USERNAME=domain\username` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops managed by vCenter Server.	None
VDM_SERVER_PASSWORD	Connection Server administrator user password. For example: `VDM_SERVER_PASSWORD=secret` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual desktops that are managed by vCenter Server.	None
VDM_IP_PROTOCOL_USAGE	Specifies the IP version that Horizon Agent uses. Valid values are IPv4 and IPv6.	IPv4

Table 15-3. MSI Properties for Silently Installing Horizon Agent (continued)

MSI Property	Description	Default Value
VDM_FIPS_ENABLED	Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will stop.	0
VDM_FORCE_DESKTOP_AGENT	If you install Horizon Agent on a Windows Server machine and configure it as a single-user Horizon desktop rather than as an RDS host, set the value to 1. This requirement applies to machines managed by vCenter Server and unmanaged machines. For non-server Windows guests that host application sessions, set the value to 0. This MSI property is optional.	0

In a silent installation command, you can use the ADDLOCAL property to specify options that the Horizon Agent installer configures.

The following table shows the Horizon Agent options that you can enter at the command line. These options have corresponding setup options that you can deselect or select during an interactive installation.

When you do not use the ADDLOCAL property at the command line, Horizon Agent installs all of the options that are installed by default during an interactive installation, if they are supported on the guest operating system. When you use ADDLOCAL=ALL, Horizon Agent installs all of the following options, both on-by-default and off-by-default, if they are supported on the guest operating system.

For more information, see the ADDLOCAL table entry in Microsoft Windows Installer Command-Line Options.

If you use ADDLOCAL to specify features individually (you do not specify ADDLOCAL=ALL), you must always specify Core.

You can modify features by using the ADDLOCAL and REMOVE MSI properties. Use the following PowerShell command to query the registry of installed components on the system where Horizon Agent is installed for the ModifyPath base command line:

```
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* |
        Select-Object DisplayName, ModifyPath | Where-Object {$_.DisplayName -eq 'VMware
Horizon
        Agent'} | Format-Table -AutoSize
```

The output:

```
DisplayName               ModifyPath
          VMware Horizon Agent      MsiExec.exe /I{A17DD662-DFB3-4997-9C0F-4E687A300111}
```

The following example modifies and removes the USB component from an existing installation: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"

The following example modifies the agent installation by replacing Horizon Performance Tracker with the Horizon Help Desk Tool: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=HelpDesk REMOVE=PerfTracker”`

The following example modifies the agent installation by adding serial port and scanner redirection: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=SerialPortRedirection,ScannerRedirection”`

Table 15-4. Horizon Agent Silent Installation Options and Interactive Custom Setup Options

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When `ADDLOCAL` Is Not Used
Core	The core Horizon Agent functions. If you specify `ADDLOCAL=ALL`, the Core features are installed.	Yes
PCoIP	PCoIP Protocol Agent	Yes
USB	USB Redirection	No
NGVC	Instant Clone Agent	No
RTAV	Real-Time Audio-Video	Yes
ClientDriveRedirection	Client Drive Redirection	Yes
SerialPortRedirection	Serial Port Redirection	No
ScannerRedirection	Scanner Redirection	No
GEOREDIR	Geolocation Redirection	No
V4V	Horizon Monitoring Service Agent	Yes
SmartCard	Smartcard This feature is not installed by default in an interactive installation.	No
VmwVaudio	VMware Audio (virtual audio driver)	Yes

Table 15-4. Horizon Agent Silent Installation Options and Interactive Custom Setup Options (continued)

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When ADDLOCAL Is Not Used
VmwVidd	VMware Indirect Display Driver	Yes **Note** VmwVidd is installed and marked as Local in the registry only if: - Desktop Mode Windows Server is RS4 and above (OS build 17134 - version 1803), `or` - Server is 19H1 and above (OS build 18362 - version 1903) VmwVidd is installed and set as `Absent` in the registry in Windows Server 2019 (version 1809) std and datacenter with the RDS role. VmwVidd will be installed and set as `Local` in the registry in Windows Server 2022 with the RDS role.
TSMMR	Windows Media Multimedia Redirection (MMR)	Yes
RDP	Enables RDP in the registry if you use the `RDP_CHOICE=1` property on the command line or select RDP as the default display protocol when you create or edit a desktop pool. This feature is hidden during interactive installations.	Yes
RDSH3D	3D rendering on RDS hosts	No
BlastUDP	UDP Transport support for Blast	Yes
SdoSensor	SDO Sensor Redirection	No
PerfTracker	Horizon Performance Tracker	No
HelpDesk	Horizon Help Desk Tool	Yes
PrintRedir	VMware Integrated Printing	Yes
PSG	This feature sets a registry entry that tells Connection Server whether Horizon Agent is using IPv4 or IPv6.	Yes

Enable Time Zone Redirection for Published Desktop and Application Sessions

If an RDS host is in one time zone and a user is in another time zone, by default, when the user connects to a published desktop, the desktop displays time that is in the time zone of the RDS host. You can enable the Time Zone Redirection group policy setting to make the published desktop display time in the local time zone. This policy setting applies to application sessions as well.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.
- Verify that the Horizon RDS ADMX files are added to Active Directory. See "Add the Remote Desktop Services ADMX Files to Active Directory" in the *Horizon Remote Desktop Features and GPOs* document.
- Familiarize yourself with the group policy settings. See " RDS Device and Resource Redirection Settings" in the *Horizon Remote Desktop Features and GPOs* document.

Procedure

1. On the Active Directory server, open the Group Policy Management Console.
2. Expand your domain and **Group Policy Objects**.
3. Right-click the GPO that you created for the group policy settings and select **Edit**.
4. In the Group Policy Management Editor, navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Device and Resource Redirection**.
5. Enable the setting **Allow time zone redirection**.

Enable Windows Basic Theme for Applications

If a user has never connected to a desktop on an RDS host, and the user launches an application that is hosted on the RDS host, the Windows basic theme is not applied to the application even if a GPO setting is configured to load the Aero-styled theme. Horizon 8 does not support the Aero-styled theme but supports the Windows basic theme. To make the Windows basic theme apply to the application, you must configure another GPO setting.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

Procedure

1. On the Active Directory server, open the Group Policy Management Console.
2. Expand your domain and **Group Policy Objects**.
3. Right-click the GPO that you created for the group policy settings and select **Edit**.
4. In the Group Policy Management Editor, navigate to **User Configuration** > **Policies** > **Administrative Templates** > **Control Panel** > **Personalization**.
5. Enable the setting **Force a specific visual style file or force Windows classic** and set the Path to Visual Style as **`%windir%\resources\Themes\Aero\aero.msstyles`**.

Configure Group Policy to Start Runonce.exe

By default, some applications that rely on the Explorer.exe file may not run in an application session. To avoid this issue, you must configure a GPO setting to start runonce.exe.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

Procedure

1. On the Active Directory server, open the Group Policy Management Console.
2. Expand your domain and **Group Policy Objects**.
3. Right-click the GPO that you created for the group policy settings and select **Edit**.
4. In the Group Policy Management Editor, navigate to **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**.
5. Double-click **Logon** and click **Add**.
6. In the Script Name box, type **`runonce.exe`**.
7. In the Script Parameters box, type **`/AlternateShellStartup`**.

RDS Host Performance Options

You can optimize Windows for either foreground programs or background services by setting performance options. By default, Horizon 8 disables certain performance options for RDS hosts for all supported versions of Windows Server.

The following table shows the performance options that are disabled by Horizon 8.

Table 15-5. Performance Options Disabled by Horizon 8

Performance Options Disabled by Horizon 8
Animate windows when minimizing and maximizing
Show shadows under mouse pointer
Show shadows under windows
Use drop shadow for icon labels on the desktop
Show windows contents while dragging

The five performance options that are disabled by Horizon 8 correspond to four Horizon 8 settings in the registry. The following table shows the Horizon 8 settings and their default registry values. The registry values are all located in the registry subkey `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`. You can re-enable the performance options by setting one or more of the Horizon 8 registry values to **`false`**.

Table 15-6. Horizon 8 Settings Related to Windows Performance Options

Horizon 8 Setting	Registry Value
Disable cursor shadow	DisableMouseShadows
Disable full window drag	DisableFullWindowDrag
Disable ListView shadow	DisableListViewShadow
Disable Window Animation	DisableWindowAnimation

RDS Host Printing Options

Horizon 8 supports both local printer redirection and native network printers.

Local printer redirection is designed for the following use cases:

- Printers directly connected to USB or serial ports on the client device.
- Specialized printers such as bar code printers and label printers connected to the client.
- Network printers on a remote network that are not addressable from the virtual session.

Network printers are managed using corporate print servers, which allows for greater management and control of printer resources. Native printer drivers for all possible printers need to be installed on the virtual machine or RDSH host. If you consider this challenging, there are third-party options such as advanced versions of ThinPrint that can provide network printing without the need to install additional printer drivers on each virtual machine or RDSH host. The Print and Document Services option included with Microsoft Windows Server is another option for managing your network printers.

When users submit print jobs concurrently from published desktops or applications that are hosted on the same RDS host, the ThinPrint server on the RDS host processes the print requests serially rather than in parallel. This can cause a delay for some users.

Configuring 3D Graphics for RDS Hosts

With 3D graphics configured for RDS hosts, both applications in application pools and applications running on published desktops can display 3D graphics.

Horizon 8 supports several 3D Graphics options for RDS hosts. Note that the options differ based whether your RDS hosts are vSphere virtual machines (automated or manual farm), non-vSphere virtual machines, or physical RDS.

3D graphics is only supported when you use the PCoIP or VMware Blast protocol. Therefore, the farm must use PCoIP or VMware Blast as the default protocol and users must not be allowed to choose the protocol.

For details on 3D graphics support for automated farm of RDS hosts using instant clones, see Configuring 3D Rendering for Automated Instant Clone Farms.

For details on 3D graphics support for manual farm of RDS hosts, see 3D Graphics Options for Manual Farms.

Understanding RDS Per-Device Client Access Licensing in Horizon

When a Windows client device connects to a published desktop or application on an RDS host, it receives an RDS Per-Device Client Access License (CAL), if the Per-Device licensing mode is configured on the RDS host.

By default, the CAL is stored only on the client device.

Note Storage of Per-Device CALs is supported only on Windows clients. Windows Zero clients, and non-Windows clients, do not support this feature. For clients that do not support this feature, CALs are stored only on the Connection Server host.

Storing the CAL makes CAL use more efficient in RDS deployments and prevents the following problems.

- If you deploy multiple license servers, and users run multiple sessions from a client device that connects to different RDS hosts that use different license servers, each license server can potentially issue a separate RDS Per-Device CAL to the same client device.

Considerations for Cloud Pod Architecture Environments

A typical Cloud Pod Architecture environment consists of multiple pods. Each pod can point to a different license server, and a single client device can use published desktops and applications on different pods in the pod federation.

If the client device has a license, it always presents that license. If the client device does not present a license, the most up-to-date license that can be found on any pod involved in the published desktop or application launch is used. If a license cannot be found on any pod involved in the launch, the client device's ID is presented to the license server and a license is issued.

Note VMware recommends that you upgrade to the latest Windows client and server software for the best handling of RDS licensing.

Creating and Managing Farms

A farm is a group of Windows Remote Desktop Services (RDS) hosts. You can create published desktops associated with a farm. You can also deliver a published application to many users by creating application pools. The published applications in application pools run on a farm of RDS hosts.

Farms simplify the task of managing RDS hosts, published desktops, and applications in an enterprise. You can create manual or automated farms to serve groups of users that vary in size or have different desktop or application requirements.

A manual farm consists of RDS hosts that already exist. The RDS hosts can be physical or virtual machines. You manually add the RDS hosts when you create the farm.

The Connection Server creates the instant clone virtual machines based on the parameters that you specify when you create the farm. Instant clones share a virtual disk of an internal parent VM and therefore consume less storage than full virtual machines. In addition, instant clones share the memory of a parent VM and are created using the vmFork technology.

Although helpful in speeding up the provisioning speed, the use of parent VM does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon automatically chooses to provision instant clones directly from replicaVM, without creating any parent VM. This feature is called Smart Provisioning. A single instant clone farm can have both instant clones that are created with parentVMs or without parent VMs.

When you create an application pool or a published desktop pool, you must specify only one farm. The RDS hosts in a farm can host published desktops, applications, or both. A farm can support at most one published desktop pool, but it can support multiple application pools. A farm can support both types of pools simultaneously. For more information on farms, see the *Horizon 8 Administration* document.

To deliver published applications on demand, you can associate a farm with an App Volumes Manager. Any host in the farm can then access the applications on the App Volumes Manager.

Creating an Automated Instant-Clone Farm

An automated farm consists of RDS hosts that are instant-clone virtual machines in vCenter Server. There is no other cloning technology available for automated farms.

An automated instant-clone farm created from a golden image using the vmFork technology (called instant clone API) in vCenter Server. Instant clone technology replaces View Composer linked clone as the process for creating automated farms in Horizon 8. In addition to using the instant clone API from vCenter Server, Horizon 8 also creates several types of internal VMs (Internal Template, Replica VM, and ParentVM) in order to manage these clones in a more scalable way.

Although helpful in speeding up the provisioning speed, the use of parentVM does increase the memory requirement across the cluster. In some cases when the benefit of having more memory outweighs the increase in provisioning speed, Horizon 8 automatically chooses to provision instant clones directly from replicaVM, without creating any parentVM. This feature is called Smart Provisioning. A single instant clone farm can have both instant clones that are created with parentVMs or without parentVMs.

When parentVM is used, instant clones share the virtual disk of the parentVM and therefore consume less storage than full VMs. In addition, instant clones share the memory of the parentVM when they are first created, which contributes to fast provisioning. Once the instant clone VM is provisioned and the machine starts to be used, additional memory is utilized.

An instant-clone desktop farm has the following benefits:

- The provisioning of instant clones is fast, with or without using parentVM.
- Instant clones are always created in a powered-on state, ready for use.

- You can patch a farm of instant clones in a rolling process with zero downtime.

Connection Server creates the instant-clone virtual machines based on the parameters that you specify when you create the farm. Instant clones share a virtual disk of a parentVM and therefore consume less storage than full virtual machines. In addition, instant clones share the memory of a parentVM and are created using the vmFork technology.

Before you create an automated instant-clone farm, you must prepare an RDS host golden image virtual machine. See Prepare an RDS Host Golden Image Virtual Machine.

Instant Clone Image Publishing and Creation Workflow for Farms

Publishing an image is a process by which internal VMs needed for instant cloning are created from a golden image and its snapshot. This process only happens once per image and may take some time.

Horizon 8 performs the following steps to create a pool of instant clones:

1. Horizon 8 publishes the image that you select. In vCenter Server, four folders (`ClonePrepInternalTemplateFolder`, `ClonePrepParentVmFolder`, `ClonePrepReplicaVmFolder`, and `ClonePrepResyncVmFolder`) are created if they do not exist, and some internal VMs that are required for cloning are created. In Horizon Console, you can see the progress of this operation on the **Summary** tab of the desktop pool. During publishing, the Pending Image pane shows the name and state of the image.

   Note Do not tamper with the four folders or the internal VMs that they contain. Otherwise, errors might occur. The internal VMs are removed when they are no longer needed. Normally the VMs are removed within 5 minutes of pool deletion or a push-image operation. However, sometimes the removal can take up to 30 minutes. If there are no internal VMs in all four folders, these folders are unprotected and you can delete these folders.

2. After the image is published, Horizon 8 creates the instant clones.. This process is fast. During this process, the Current Image pane in Horizon Console shows the name and state of the image.

After the farm is created, you can change the image through the push-image operation. As with the creation of a farm, the new image is first published. Then the clones are recreated.

When an instant clone pool farm is created, Horizon 8 spreads the pool across datastores automatically in a balanced way. If you edit a farm to add or remove datastores, rebalancing of the cloned VMs happens automatically when a new clone is created.

Preparing a Golden Image Virtual Machine for an Automated Farm

To create an automated farm, you must first prepare a golden image virtual machine. Connection Server uses this golden image virtual machine to create instant-clone virtual machines, which are the RDS hosts in the farm.

What to read next

- Prepare an RDS Host Golden Image Virtual Machine

  Connection Server requires a golden image virtual machine from which you generate a base image for creating instant clones.

- Deactivate Windows Hibernation in the Golden Image

  The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Deactivating hibernation reduces the size of an instant clone's virtual disk.

Prepare an RDS Host Golden Image Virtual Machine

Connection Server requires a golden image virtual machine from which you generate a base image for creating instant clones.

Prerequisites

- Verify that an RDS host virtual machine is set up. See Setting Up Remote Desktop Services Hosts. To set up the RDS host, be sure not to use a virtual machine that was previously registered to Connection Server.
- To create an automated instant-clone farm, you must select the **Instant Clone** option when you install Horizon Agent on the golden image virtual machine. See Install Horizon Agent on a Remote Desktop Services Host.
- Verify that the virtual switch that the instant-clone VMs connect to has enough ports to support the expected number of VMs. Each network card on a VM requires one port.
- Verify that you added an instant-clone domain administrator in Horizon Console. See *Add an Instant-Clone DomainAdministrator* in the *Horizon 8 Installation and Upgrade* document.
- To deploy Windows machines, configure a volume license key and activate the golden image virtual machine's operating system with volume activation.
- Familiarize yourself with the procedure for disabling searching Windows Update for device drivers. See the Microsoft Technet article, "Disable Searching Windows Update for Device Drivers" at http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx.
- To implement the RDS host load balancing feature, modify the RDS host golden image virtual machine.

Procedure

◆ Verify that the system disk contains a single volume.

◆ Verify that the virtual machine does not contain an independent disk.

  An independent disk is excluded when you take a snapshot of the virtual machine.

◆ Before you take a snapshot of the golden image virtual machine, disable searching Windows Update for device drivers.

- In vSphere Client, disable the vApp Options setting on the golden image virtual machine.

What to do next

Use vSphere Client to take a snapshot of the golden image virtual machine in its powered-down state.

Important Before you take a snapshot, completely shut down the golden image virtual machine by using the **Shut Down** command in the guest operating system.

Deactivate Windows Hibernation in the Golden Image

The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Deactivating hibernation reduces the size of an instant clone's virtual disk.

Caution When you make hibernation unavailable, hybrid sleep does not work. Users can lose data if a power loss occurs.

Procedure

1. In vSphere Client, select the golden image virtual machine and select **Open Console**.
2. Log in as an administrator.
3. Deactivate the hibernation option.
   a. Click **Start** and type **`cmd`** in the **Start Search** box.
   b. In the search results list, right-click **Command Prompt** and click **Run as Administrator**.
   c. At the **User Account Control** prompt, click **Continue**.
   d. At the command prompt, type **`powercfg.exe /hibernate off`** and press Enter.
   e. Type **`exit`** and press Enter.

Worksheet for Creating an Automated Instant-Clone Farm in Horizon

When you create an automated instant-clone farm, you can configure certain settings.

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm.	
Description	Description of this farm.	
Access group	Select an access group for the farm, or leave the farm in the default root access group.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Default display protocol	Select **VMware Blast**, **PCoIP** or **Microsoft RDP**. Microsoft RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **Microsoft RDP** and you plan to use this farm to host application pools, you must set **Allow users to choose protocol** to **Yes**. The default is **PCoIP**.	
Allow users to choose protocol	Select **Yes** or **No**. This setting applies to published desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to a published desktop from Horizon Client. The default is **Yes**.	
3D Renderer	Select 3D graphics rendering for desktops. NVIDIA GRID vGPU is the only 3D rendering option offered for automated farm of instant clone RDS hosts.	
Pre-launch session timeout (applications only)	Determines the amount of time that an application configured for pre-launch is kept open. The default is **10 minutes**. If the end-user does not start any application in Horizon Client, the application session is disconnected if the idle session times out or if pre-launch session times out. If you want to end the pre-launch session after timeout, you must set the **Log off disconnected session** option to **Immediate**.	
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select **Never**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select **Immediate**, the session logs you out or disconnects within 30 seconds. You can further reduce the time the session logs out or disconnects by editing a registry key on a Windows RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged off frees up resources, but opening an application takes longer. The default is **Disconnect**.	
Log off disconnected sessions	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select **Never**, **Immediate**, or **After ... minutes**. Use caution when you select **Immediate** or **After ... minutes**. When a disconnected session is logged off, the session is lost. The default is **Never**.	
Bypass Session Timeout	Enable this setting to allow application sessions to run forever. Application sessions that run forever are supported on Windows and Linux clients. This setting is not available for application pools in a cloud pod architecture environment. Application sessions that run forever are not supported for unauthenticated users. Do not enable this setting if the max session timeout value is set to **Never**. When you restart Connection Server, existing forever running application sessions no longer run indefinitely.	
Allow Session Collaboration	Select **Enabled** to allow users of desktop pools based on this farm to invite other users to join their remote desktop sessions. Session owners and session collaborators must use the VMware Blast display protocol.	
Max sessions per RDS Host	Determines the maximum number of sessions that an RDS host can support. Select **Unlimited** or **No More Than ...**. The default is **Unlimited**.	
Load Balancing	See Load Balancing Settings for the list of settings.	
Enable provisioning	Select this checkbox to enable provisioning after you finish this wizard. This box is checked by default.	
Stop provisioning on error	Select this checkbox to stop provisioning when a provisioning error occurs. This box is checked by default.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Naming pattern	Specify a prefix or a name format. Horizon 8 will append or insert an automatically generated number starting with 1 to form the machine name. If you want the number at the end, simply specify a prefix. Otherwise, specify **{n}** anywhere in a character string and **{n}** will be replaced by the number. You can also specify **{n:fixed=<number of digits>}**, where **fixed=<number of digits>** indicates the number of digits to be used for the number. For example, specify **vm-{n:fixed=3}-sales** and the machine names will be vm-001-sales, vm-002-sales, and so on. **Note** Each machine name, including the automatically generated number, has a 15-character limit.	
Max number of machines	The number of machines to be provisioned.	
Minimum number of ready (provisioned) machines during Instant Clone maintenance operations	This setting lets you keep the specified number of machines available to accept connection requests while Connection Server performs maintenance operations on the machines in the farm. This setting is not honored if you schedule immediate maintenance.	
Use VMware vSAN	Specify whether to use VMware vSAN, if available. vSAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts.	
Select separate datastores for replica and OS disks	(Available only if you do not use vSAN) You can place replica and OS disks on different datastores for performance or other reasons. If you select this option, you can select the options to select one or more instant-clone datastores or replica disk datastores.	
Golden image	Select a golden image virtual machine from the list.	
Snapshot	Select the snapshot of the golden image virtual machine to use as the base image for the farm. Do not delete the snapshot and golden image virtual machine from vCenter Server, unless no instant clones in the farm use the default image, and no more instant clones will be created from this default image. The system requires the golden image virtual machine and snapshot to provision new instant clones in the farm, according to farm policies. The golden image virtual machine and snapshot are also required for Connection Server maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the farm resides.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Cluster	Select the ESXi host or cluster on which the desktop virtual machines run. For the maximum limit on the cluster, see the KB article on Sizing Limits and Recommendations.	
Resource pool	Select the vCenter Server resource pool in which the farm resides.	
Datastores	Select one or more datastores on which to store the farm. A table on the **Select Instant Clone Datastores** page of the Add Farm wizard provides high-level guidelines for estimating the farm's storage requirements. These guidelines can help you determine which datastores are large enough to store the instant-clones. The Storage Overcommit value is always set to Unbounded and is not configurable. **Note** If you use vSAN, there is only one datastore.	
Replica disk datastores	Select one or more replica disk datastores on which to store the instant-clones. This option appears if you select separate datastores for replica and OS disks. A table on the **Select Replica Disk Datastores** page of the Add Farm wizard provides high-level guidelines for estimate the farm's storage requirements. These guidelines can help you determine which replica disk datastores are enough to store the instant-clones.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Networks	**Note** If the selected Golden Image has multiple network adapters, the wizard shows a selection grid for each adapter. To change the number of adapters, make the change on the Instant Clone Golden Image, and select that Golden Image to use for the new pool. If the selected Golden Image has multiple network adapters, the wizard selects the network type of Adapter 1 as the network type. To change the network type for the Golden Image, edit the network type on the Instant Clone Golden Image, and select that Golden Image to use for the new pool. Select the networks to use for the automated instant-clone farm. You can select multiple vLAN networks to create a larger instant-clone desktop farm. The default setting uses the network from the Golden Image selected. The **Select Networks** wizard provides a list of networks based on the Golden Image's preferred network adapter (Network Adapter 1) network type: Standard, NSX Opaque Network, NSX-V, CVDS, 4.x+ and DVS. To use multiple networks, you must deselect **Use network from golden image** (which selects the network and network type from the selected Golden Image) and then select the networks to use with the instant-clone farm. The **Show all networks for each network adapter** switch shows or hides (greys out) incompatible networks for all network types. By default, only compatible networks are shown. If you select an incompatible network, such as vmcNetworks, you see this error message: **This network belongs to VMC internal network**. **Note** You can select any one available Standard Network per network adapter for Instant Clone farms. It is not supported to use more than one Standard Network per network adapter. The wizard also provides the list of ports and port bindings that are available to use: static (early binding) and ephemeral. All selected NSX-T or VDS network segments must be the same size, such as all /24 networks. Unequal sized segments can result in provisioning errors. The wizard displays error messages for the following incompatible networks: ■ **vmcNetworks**. This network belongs to VMC internal network ■ **dvsUplinkPort**. Cannot use network because it does not meet the naming standards for a virtual switch uplink port.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
	■ **notConfiguredOnAllHosts**. Cannot use network because it is not configured on all hosts in the cluster. See https://kb.vmware.com/s/article/90569 for additional information.	
CPU	Update the default CPU if desired. ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. **Note** The CPU value must be a multiple of the Cores per Socket value.	
RAM	Update the default RAM if desired. ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function. **Note** If you set a memory reservation on the Golden Image VM through vSphere Client, use the "Reserve all guest memory (All locked)" option to ensure the correct behavior when creating pools with different amounts of RAM than the Golden Image.	
Cores per Socket	Update the default Cores per Socket if desired. ■ The default value is taken from the selected snapshot in vCenter. ■ You can update this value again in the future using the Push Image function.	
Domain	Select the Active Directory domain and user name. Connection Server requires certain user privileges to farm. The domain and user account are used by ClonePrep to customize the instant-clone machines. You specify this user when you configure Connection Server settings for vCenter Server. You can specify multiple domains and users when you configure Connection Server settings. When you use the **Add Farm** wizard to create a farm, you must select one domain and user from the list.	
AD container	Provide the Active Directory container relative distinguished name. For example: `CN=Computers` When you run the **Add Farm** wizard, you can browse your Active Directory tree for the container. You can cut, copy, or paste in the container name.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Allow reuse of pre-existing computer accounts	Select this option to use existing computer accounts in Active Directory when the virtual machine names of new instant clones match the existing computer account names. When an instant clone is created, if an existing AD computer account name matches the instant-clone virtual machine name, Horizon 8 uses the existing computer account. Otherwise, a new computer account is created. The existing computer accounts must be located in the Active Directory container that you specify with the AD container setting. When this option is disabled, a new AD computer account is created when Horizon 8 creates an instant clone. This option is disabled by default.	
Image Publish Computer Account	Publishing instant-clones requires an additional computer account in the same AD domain as the clones. If you want to use pre-created computer accounts instead of auto-created computer accounts, you must also create the additional computer account and specify its name here. Then you do not need to delegate Create and Delete of computer objects to the provisioning account.	

Table 15-7. Worksheet: Configuration Settings for Creating an Automated Instant-Clone Farm (continued)

Setting	Description	Fill in Your Value Here
Use ClonePrep or a customization specification (Sysprep)	Choose whether to use ClonePrep or select a customization specification (Sysprep) to configure licensing, domain attachment, DHCP settings, and other properties on the machines. ■ **Power-off script name**. Name of the customization script that ClonePrep runs on instant-clone machines before they are powered off. Provide the path to the script on the golden image virtual machine. ■ **Power-off script parameters**. Provide parameters that ClonePrep can use to run a customization script on instant-clone machines before they are powered off. For example, use p1. ■ **Post-synchronization script name**. Name of the customization script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. Provide the path to the script on the golden image virtual machine. ■ **Post-synchronization script parameters**. Provide parameters for the script that ClonePrep runs on instant-clone machines after they are created or an image has been pushed to them. For example, use p2. After you use ClonePrep or Sysprep when you create a farm, you cannot switch to the other customization method later on, when you create or recompose machines in the farm. After you use ClonePrep or Sysprep when you create a farm, you can edit the customization type or spec name. Changes to the customization spec are not reflected on the farm until a new push image is scheduled, and the currently published image continues to use the old spec even if it has been edited or deleted. If push image fails, the farm continues using the old unedited spec. However, the farm settings continue to point to the new spec name if it has been changed. For more information about the differences between ClonePrep and Sysprep, see Choosing ClonePrep or Sysprep for Customizing Your Windows Virtual Desktops.	
Ready to Complete	Review the settings for the automated instant-clone farm.	

Create an Automated Instant-Clone Farm in Horizon

You create an automated instant-clone farm as part of the process to give users access to published applications or published desktops.

Prerequisites

- Verify that Connection Server is installed. See the *Horizon 8 Installation and Upgrade* document.
- Verify that Connection Server settings for vCenter Server are configured in Horizon Console. See the *Horizon 8 Administration* document.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools.
- Verify that you prepared a golden image virtual machine. Horizon Agent must be installed on the golden image virtual machine. See Preparing a Golden Image Virtual Machine for an Automated Farm.
- Take a snapshot of the golden image virtual machine in vCenter Server. You must shut down the golden image virtual machine before you take the snapshot. Connection Server uses the snapshot as the base image from which the clones are created.
- Gather the configuration information you must provide to create the farm. See Worksheet for Creating an Automated Instant-Clone Farm in Horizon.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Click **Add**.
3. Select **Automated Farm**.
4. Select **Instant clone**.
5. Follow the prompts in the wizard to create the farm.

   Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

   Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

   - If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
   - If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken.

   For more information, see the VMware Carbon Black Cloud Documentation. For best practices on using Carbon Black with VMware Horizon 8, see VMware Knowledge Base (KB) article 95512.

What to do next

For published applications or desktops, create a published application pool or a published desktop pool. See Create an Application Pool or Create a Published Desktop Pool.

For published applications on demand, associate the RDS farm with an App Volumes Manager. See Associate App Volumes Manager with a Farm.

Configuring 3D Rendering for Automated Instant Clone Farms

When you create or edit a farm of instant clone RDS machines, you can configure 3D graphics rendering for your farm. Instant clone farms support NVIDIA GRID vGPU for 3D rendering.

Horizon 8 does not directly control settings for 3D rendering of an instant-clone farm as it does with full-clone virtual machines. You need to configure 3D settings in the ESXi hosts, and then in your golden image using the vSphere Client. Instant-clone virtual machines will inherit those settings from the golden image. Horizon Console will display some of the settings you configured, but you cannot edit or interact with those settings.

The ESXi host assigns GPU hardware resources to virtual machines on a first-come, first-served basis as virtual machines are created. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is the **best performance** mode. If you would rather have the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU, you can use the **GPU consolidation** mode. You can configure this mode in vCenter Server for each ESXi host that has vGPU installed. For more information, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/55049.

If you are only using a single vGPU profile per vSphere cluster, set the GPU assignment policy for all GPU hosts within the cluster to the **best performance** mode in order to maximize performance. In this case, you can also have instant-clone pools and full-clone pools that use the same vGPU profile in the same vSphere cluster.

You can have a cluster with some GPU enabled hosts and some non-GPU enabled hosts.

NVIDIA GRID vGPU has these potential constraints:

- RDP is not supported.
- The virtual machines must be hardware version 11 or later.
- vMotion of a VM between vGPU-enabled hosts is supported starting with vSphere 6.7. You cannot use vSphere Distributed Resource Scheduler (DRS) with vGPU.
- Horizon 8 does support creating a vGPU instant-clone farm using a cluster with some vGPU enabled hosts and non-vGPU enabled hosts, and will just ignore the non-vGPU enabled hosts when creating the farm. You can not use vMotion to move an instant-clone from a GPU-enabled ESXi host to an ESXi host that does not have GPU hardware configured.

To enable an instant-clone farm to use NVIDIA GRID vGPU:

Procedure

1 Install NVIDIA GRID vGPU in the physical ESXi hosts.

2 In vCenter Server hardware graphics configuration, select the Host Graphics tab, and in **Edit Host Graphics Settings**, select **Shared Direct**.

   ESXi host uses the NVIDIA GRID card for vGPU.

3 Prepare a golden image with NVIDIA GRID vGPU configured, including selecting the vGPU profile you want to use.

4 Take a snapshot of the golden image.

5 In Horizon Console, when you create an instant-clone farm, select this golden image and snapshot.

Results

Horizon 8 automatically displays **NVIDIA GRID vGPU** in the 3D Render field. Horizon 8 also displays the vGPU profile you chose in the golden image. Instant clones inherit the settings configured in the vSphere Client for the golden image.

The vGPU profile cannot be edited from Horizon Console during the instant-clone farm creation process, To edit the vGPU profile for a farm once the farm has been created, you can create a new image with the updated vGPU profile, take a snapshot, and then do a push-image operation.

Creating a Manual Farm

A manual farm consists of RDS hosts that already exist. The RDS hosts can be physical, vSphere virtual machines (excluding instant clones), or non-vSphere virtual machines. You manually add the RDS hosts when you create the farm.

Before you create a manual farm, you must prepare existing RDS hosts for Horizon 8. See Setting Up Remote Desktop Services Hosts.

Worksheet for Creating a Manual Farm in Horizon

When you create a manual farm, you can configure certain farm settings.

Table 15-8. Worksheet: Configuration Settings for Creating a Manual Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm.	
Description	Description of this farm.	
Access group	Select an access group for the farm, or leave the farm in the default root access group.	

Table 15-8. Worksheet: Configuration Settings for Creating a Manual Farm (continued)

Setting	Description	Fill in Your Value Here
Default display protocol	Select **VMware Blast**, **PCoIP** or **Microsoft RDP**. Microsoft RDP applies to desktop pools only. The display protocol for application pools is always **VMware Blast** or **PCoIP**. If you select **Microsoft RDP** and you plan to use this farm to host application pools, you must set **Allow users to choose protocol** to **Yes**. The default is **PCoIP**.	
Allow users to choose protocol	Select **Yes** or **No**. This setting applies to published desktop pools only. If you select **Yes**, users can choose the display protocol when they connect to a published desktop from Horizon Client. The default is **Yes**.	
Pre-launch session timeout (applications only)	Determines the amount of time that an application configured for pre-launch is kept open. The default is **10 minutes**. If the end-user does not start any application in Horizon Client, the application session is disconnected if the idle session times out or if pre-launch session times out. If you want to end the pre-launch session after timeout, you must set the **Log off disconnected session** option to **Immediate**.	
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log out from empty application sessions. Select **Never**, **Immediate**, or set the number of minutes as the timeout value. The default is **After 1 minute**. If you select **Immediate**, the session logs you out or disconnects within 30 seconds. You can further reduce the time the session logs out or disconnects by editing a registry key on a Windows RDS Host on which Horizon Agent is installed. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params` and set a value for `WindowCheckInterval`. The default value is 20000. This means that the poll for the empty session check is every 20 seconds, which sets the maximum time between the last application session close and session logout to 40 seconds. You can change this value to 2500. This means that the poll for the empty session check is every 2.5 seconds, which sets the maximum time between the last application close and session logout to 5 seconds.	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the **Empty session timeout** limit is reached. Select **Disconnect** or **Log off**. A session that is logged off frees up resources, but opening an application takes longer. The default is **Disconnect**.	
Log off disconnected sessions	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select **Never**, **Immediate**, or **After ... minutes**. Use caution when you select **Immediate** or **After ... minutes**. When a disconnected session is logged off, the session is lost. The default is **Never**.	

Table 15-8. Worksheet: Configuration Settings for Creating a Manual Farm (continued)

Setting	Description	Fill in Your Value Here
Bypass Session Timeout	Enable this setting to allow application sessions to run forever. Application sessions that run forever are supported on Windows and Linux clients. This setting is not available for application pools in a cloud pod architecture environment. Application sessions that run forever are not supported for unauthenticated users. Do not enable this setting if the max session timeout value is set to **Never**. When you restart Connection Server, existing forever running application sessions no longer run indefinitely.	
Allow Session Collaboration	Select **Enabled** to allow users of desktop pools based on this farm to invite other users to join their remote desktop sessions. Session owners and collaborators must use the VMware Blast protocol.	
Use custom script	Select this setting to use a custom script for load balancing. If this setting is enabled, Horizon 8 does not consider other load balancing settings and reads the `CustomLoadValue` registry key in the following location to get the server load index: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. See, Writing a Load Balancing Script for an RDS Host.	
Include session count	Select this setting to include the session count on the RDS host for load balancing. If none of the settings are selected for load balancing and if the custom script setting is not selected, Horizon 8 uses the session count by default. Disable this setting if you do not need to consider the session count for load balancing.	
Select RDS Hosts	Select the RDS host from the list.	
CPU usage threshold	Threshold value for the CPU usage in percentage. Horizon 8 uses the configured CPU threshold to calculate the CPU load index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.	
Memory usage threshold	Threshold value for the memory in percentage. Horizon 8 uses the configured memory threshold to calculate the Memory Load Index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.	
Disk queue length threshold	Threshold of the average number of both read and write requests that were queued for the selected disk during the sample interval. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing.	

Table 15-8. Worksheet: Configuration Settings for Creating a Manual Farm (continued)

Setting	Description	Fill in Your Value Here
Disk read latency threshold	Threshold of the average time of read of data from the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.	
Disk write latency threshold	Threshold of the average time of write of data to the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.	

Create a Manual Farm in Horizon

Create a manual farm as part of the process to give users access to published applications or desktops.

Prerequisites

- Set up the RDS hosts that belong to the farm. See Setting Up Remote Desktop Services Hosts.
- Verify that all the RDS hosts have the Available status. In Horizon Console, select **Settings > Registered Machines** and check the status of each RDS host on the RDS Hosts tab.
- Gather the configuration information you must provide to create the farm. See Worksheet for Creating a Manual Farm in Horizon.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Click **Add**.

3 Select **Manual Farm**.

4 Follow the prompts in the wizard to create the farm.

Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page by clicking the page name in the navigation pane.

5 Select the RDS hosts to add to the farm and click **Next**.

6 Click **Finish**.

What to do next

Create a published application or desktop pool.

Associate App Volumes Manager with a Farm

For published applications on demand, you must associate an App Volumes Manager with an automated instant-clone farm. Applications on the App Volumes Manager can be published from any host on that farm.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Select the farm you want to associate and click **More Commands > Associate App Volumes Manager**.
3. Select the App Volumes Manager that manages the farm and click **OK**.

Unassociate App Volumes Manager

You can unassociate an App Volumes Manager from a farm after deleting all application pools from that farm.

Prerequisites

Delete the applications published from the App Volumes Manager.

Procedure

1. In Horizon Console, navigate to **Inventory > Farms** and select a farm
2. Click **More Commands > Unassociate App Volumes Manager** and click **OK**.

Results

The App Volumes Manager's farm association is removed from the Horizon Console.

3D Graphics Options for Manual Farms

3D graphics options are available for a manual farm of RDS using vSphere virtual machines.

These options are applicable to vSphere virtual machines. If you have a manual farm of non-vSphere virtual machines or physical servers, you can leverage GPU capabilities that are available to the OS.

NVIDIA GRID vGPU (shared GPU hardware acceleration)

A physical GPU on an ESXi host is shared among multiple virtual machines.

AMD Multiuser GPU using vDGA

A physical GPU on an ESXi host is shared among multiple virtual machines.

Virtual Dedicated Graphics Acceleration (vDGA)

A physical GPU on an ESXi host is dedicated to a single virtual machine.

Note See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

3D graphics is only supported when you use the PCoIP or VMware Blast protocol. Therefore, the farm must use PCoIP or VMware Blast as the default protocol and users must not be allowed to choose the protocol.

With vDGA, you allocate an entire GPU to a single machine for maximum performance. The RDS host must be in a manual farm.

With AMD Multiuser GPU using vDGA, you can share an AMD GPU between multiple RDS hosts by making it appear as multiple PCI passthrough devices. The RDS host must be in a manual farm.

With NVIDIA GRID vGPU, each graphics card can support multiple RDS hosts or virtual machines. If an ESXi host has multiple physical GPUs, you can also configure the way the ESXi host assigns virtual machines to the GPUs. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is called performance mode. You can also choose consolidation mode, where the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU. To configure consolidation mode, edit the `/etc/vmware/config` file on the ESXi host and add the following entry:

```
vGPU.consolidation = "true"
```

Overview of Steps for Configuring 3D Graphics

This overview describes tasks that you must perform in vSphere and Horizon 8 to configure 3D graphics.

1 Set up an RDS host virtual machine. For more information, see Setting Up Remote Desktop Services Hosts.

2 Add the graphics PCI device to the virtual machine. See "Other Virtual Machine Device Configuration" in the chapter "Configuring Virtual machine Hardware" in the *vSphere Virtual Machine Administration* document. Be sure to click **Reserve all memory** when adding the device.

3 On the virtual machine, install the device driver for the graphics card.

4 Add the RDS host to a manual farm, create a published desktop pool, connect to the desktop using PCoIP, and activate the display adapter.

You do not need to configure 3D graphics for RDS hosts in Horizon Console. Selecting the option **3D RDSH** when you install Horizon Agent is sufficient. By default, this option is not selected and 3D graphics is disabled.

Managing Farms

In Horizon Console, you can add, edit, delete, enable, and disable farms.

After you create a farm, you can add or remove RDS hosts to support more or fewer users.

Edit a Farm

For an existing farm, you can make changes to the configuration settings.

Prerequisites

Familiarize yourself with the settings of a farm.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Select a farm and click **Edit**.

3 Make changes to the farm settings.

4 Click **OK**.

Delete a Farm

You can delete a farm if you no longer need it or if you want to create a new one with different RDS hosts. You can only delete a farm that is not associated with published desktop or application pool.

Prerequisites

Verify that the farm is not associated with any published desktop pool or application pool.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Select one or more farms and click **Delete**.

3 Click **OK** to confirm.

Disable or Enable a Farm

When you disable a farm, users can no longer launch published desktops or applications from the published desktop pools and the application pools that are associated with the farm. Users can continue to use published desktops and applications that are currently open.

You can disable a farm if you plan to do maintenance on the RDS hosts in the farm or on the published desktop and application pools that are associated with the farm. After you disable a farm, some users might still be using published desktops or applications that they opened before you disable the farm.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Select one or more farms and click **More Commands**.

3 Click **Enable** or **Disable**.

4 Click **OK** to confirm.

Results

You can view the status of the pools by selecting **Inventory > Desktops** or **Inventory > Applications**.

Schedule Maintenance for an Automated Instant-Clone Farm in Horizon

With the maintenance operation, you can schedule recurring or immediate maintenance of all the RDS hosts in an automated instant-clone farm. During each maintenance cycle, all the RDS hosts are refreshed from the golden image virtual machine. Depending on how you want the golden image to be managed, you can change the golden image and snapshot source in your pool from vCenter to Image Catalog or reverse. For more information on the Image Management Service, see the *Managing Horizon Images from the Cloud* document.

You can make changes to the golden image virtual machine without affecting the RDS host instant clones because the snapshot of the current golden image VM is used for maintenance. The instant clones created in the automated farm use the information in the golden image VM for their system configuration.

If possible, schedule maintenance operations during off-peak hours to ensure all that RDS hosts have finished maintenance and are available during peak hours.

Note When scheduling maintenance and selecting to wait for users to log off, Horizon will automatically disable RDS Hosts (preventing new connections) as required in order to allow sessions to drain and maintenance to occur. The minimum farm size setting is honored, meaning that number of RDS Hosts will remain available for new connections.

Prerequisites

- Decide when to schedule the maintenance operation. By default, Connection Server starts the operation immediately.

  You can schedule an immediate maintenance or recurring maintenance or both for a farm. You can schedule maintenance operations on multiple farms concurrently.

- Decide whether to force all users to log off when the maintenance operation begins or wait for all users to log off an RDSH before refreshing that RDSH machine.

  If you force users to log off, Horizon 8 notifies users before they are disconnected and allows them to close their applications and log off.

- Decide the minimum farm size. The minimum farm size is the number of RDS hosts that are kept available at all times to allow users to continue to use the farm. For example, if the farm size is ten and the minimum farm size is two, then maintenance will be performed on eight RDS hosts. As each RDS host becomes available again then the remaining hosts will go through maintenance. All RDS hosts are managed individually, so as one host becomes available then one of the remaining hosts will be put into maintenance.

However, if you schedule immediate maintenance, then all the RDS hosts in the farm will be put into maintenance.

All RDS hosts will also be subject to policy and will wait for logoff or force users to logoff depending upon what policy is configured.

- Decide whether to stop provisioning at first error. If you select this option and an error occurs when Connection Server provisions an instant-clone, provisioning stops. You can select this option to ensure that resources such as storage are not consumed unnecessarily.

  Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on an instant-clone, other clones continue to be provisioned and customized.
- Verify that provisioning is enabled. When provisioning is disabled, Horizon 8 stops the machines from being customized after they are refreshed.
- If your deployment includes replicated Connection Server instances, verify that all instances are the same version.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Click the pool ID of the farm for which you want to schedule a maintenance.
3. Click **Maintain > Schedule**.

4 In the **Schedule Recurring Maintenance** wizard, choose a maintenance mode.

◆

Option	Action
Recurring	Schedules periodic maintenance of all the RDS host servers in a farm. ■ Select a date and time from which the maintenance is effective. ■ Select a maintenance period. You can select daily, monthly, or weekly maintenance periods. ■ Select a repeat interval in days for the maintenance operation to recur. If an immediate maintenance is scheduled on a farm, then the immediate maintenance date becomes the effective date for any recurring maintenance. If you cancel the immediate maintenance, then the current date becomes the effective date for recurring maintenance.
Immediate	Schedules immediate maintenance of all the RDS host servers in a farm. Immediate maintenance creates a one-time maintenance schedule for immediate or near future maintenance. Use immediate maintenance to refresh the farm from a new image when you want to apply urgent security patches. Select an immediate maintenance configuration. ■ Select **Start Now** to start the maintenance operation instantly. ■ Select **Start at** to start the maintenance operation at a near future date and time. Enter the date and Web browser local time. **Note** Recurring maintenance will be put on hold until immediate maintenance is complete.
Publish Secondary Image	The image you used to create a pool is the default image. By default, all maintenance operations use this image to update all machines in the farm. You can optionally publish a secondary image, which you can use to update a subset of the machines in the farm while leaving the rest unchanged. After you have published the secondary image, options are enabled to apply either of the images to selected machines without using the **Schedule Recurring Maintenance** process. ■ To apply the secondary image, select the machines on the **RDS Hosts** tab of the Farms page and then select **More Commands > Apply Secondary Image**. ■ To apply the default image, select the machines on the **RDS Hosts** tab of the Farms page and then select **More Commands > Apply Default Image**.

Option	Action
	If the new image meets your acceptance criteria, you can promote this secondary image to be your default image. Otherwise, you can cancel the secondary image and the default image will get applied to the desktop pool. ■ There is an option on the **Summary** tab to promote the secondary image. This causes the secondary image to become the new default image on the pool and applies it to all the machines in the pool. To promote the secondary image, select **Maintain > Promote Secondary Image**. ■ To cancel the secondary image, select **Maintain > Cancel** on the **Summary** tab. ■ If the pool is set to refresh on logoff, the desktops that are currently on the secondary image will revert to the default image once the user logs off. ■ If the pool is not set to refresh on logoff, the desktops on the secondary image remain on it unless a recover, delete, or refresh is performed on the desktop.

5 Click **Next**.

6 (Optional) Click **Change** to change the golden image virtual machine. You can change the image source from vCenter to Image Catalog or vice versa.

7 Select a snapshot.

You cannot select a different snapshot unless you clear the **Use current parent VM image** checkbox. Click **Snapshot Details** to display details about the snapshot. If the image source is Image Catalog, select the required stream and marker.

Note If you are a VMware Carbon Black customer and select a golden image configured with Carbon Black, then the screen displays information from the Carbon Black Scan for each snapshot listed.

- If you select the Show All Images check box, the list might include snapshots that are not compatible and cannot be selected.
- If no value appears in the Carbon Black Scan (% Complete) column, that indicates that the Carbon Black sensor was not enabled in the Instant Clone golden image when the snapshot was taken.

For more information, see the VMware Carbon Black Cloud Documentation. For best practices on using Carbon Black with VMware Horizon 8, see VMware Knowledge Base (KB) article 95512.

8 Click **Next**.

9 (Optional) Specify whether to force users to log off or wait for users to log off.

The option to force users to log off is selected by default.

10 (Optional) Specify whether to stop provisioning at first error.

This option is selected by default.

11 Click **Next**.

The **Ready to Complete** page is displayed.

12 Click **Finish**.

Creating Published Desktop Pools

One of the tasks that you perform to give users remote access to session-based desktops is to create a published desktop pool. A published desktop pool runs on a farm of RDS hosts and has properties that can satisfy some specific needs of a remote desktop deployment.

Understanding Published Desktop Pools

An published desktop pool is one of three types of desktop pools that you can create. This type of pool was known as a Microsoft Terminal Services pool in previous Horizon 8 releases.

A published desktop pool and a published desktop have the following characteristics:

- A published desktop pool is associated with a farm, which is a group of RDS hosts. The farm can be an automated farm or a manual farm. Each RDS host is a Windows server that can host multiple published desktops.
- A published desktop is based on a session to an RDS host. In contrast, a desktop in an automated desktop pool is based on a virtual machine, and a desktop in a manual desktop pool is based on a virtual or physical machine.
- A published desktop supports the RDP, PCoIP, and VMware Blast display protocols.
- A published desktop pool is only supported on Windows Server operating systems that support the RDS role and are supported by Horizon 8. See "System Requirements for Guest Operating Systems" in the *Horizon 8 Installation and Upgrade* document.
- Horizon 8 provides load balancing of the RDS hosts in a farm by directing connection requests to the RDS host that has the least number of active sessions.

Published Desktop Pools Settings

You can specify certain pool settings when you create an published desktop pool that run on a farm of RDS hosts. Not all pool settings apply to all types of desktop pools. These settings are specific to published desktop pools.

Table 15-9. Settings for a Published Desktop Pool

Setting	Description	Default Value
State	■ **Enabled**. After being created, the desktop pool is enabled and ready for immediate use. ■ **Disabled**. After being created, the desktop pool is disabled and unavailable for use, and provisioning is stopped for the pool. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance. When this state is in effect, remote desktops are unavailable for use.	Enabled
Connection Server restrictions	You can restrict access to the desktop pool to certain Connection Servers by clicking **Browse** and selecting one or more Connection Servers. If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager application might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.	None
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the desktop pool entitlement on Windows client devices.	Disabled
Client Restrictions	Select whether to restrict access to entitled desktop pools from certain client computers. You must add the names of the computers that are allowed to access the desktop pool in an Active Directory security group. You can select this security group when you add users or groups to the desktop pool entitlement.	Disabled

Table 15-9. Settings for a Published Desktop Pool (continued)

Setting	Description	Default Value
Allow user to initiate separate sessions from different client devices	When you enable this setting, users that connect to the same desktop pool from different client devices receive different desktop sessions. To reconnect to an existing desktop session, users must use the same device from which that session was initiated. If you do not select this setting, users are always reconnected to their existing desktop sessions, regardless of the client device that they use. The RDP display protocol is not supported if you select this setting. Default is **No**. **Note** If you enable this policy, all the desktop pools in the global entitlement must also support multiple sessions per user. For more information about understanding the multiple sessions per user policy for global desktop entitlements, see the *Cloud Pod Architecture in Horizon 8* document.	
Allow Machine Name Selection	Enabling this option will allow a command line launch of Horizon Client to specify a machine name to connect to, for example for test or troubleshooting purposes.	

Create a Published Desktop Pool

You create a published desktop pool as part of the process to give users access to desktops that run on a farm of RDS hosts.

Prerequisites

- Set up RDS hosts. See Setting Up Remote Desktop Services Hosts.
- Create a farm that contains the RDS hosts. See Creating and Managing Farms.
- Decide how to configure the pool settings. See Published Desktop Pools Settings.

Procedure

1 In Horizon Console, select **Inventory > Desktops**.

2 Click **Add**.

3 Select **RDS Desktop Pool** and click **Next**.

4 Provide a pool ID, display name, and description.

The pool ID is the unique name that identifies the pool in Horizon Console. The display name is the name of the published desktop pool that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as the pool ID.

5 Select pool settings.

6 Select an existing farm or create a farm for this pool.

What to do next

Entitle users to access the pool.

If you have connected your pod to Horizon Cloud and want information on configuring published desktop pools for use in a Universal Broker environment, see Horizon Pods - Configure RDSH Desktops and Applications for a Universal Broker Environment.

Troubleshooting Internal Virtual Machines in Instant-Clone Desktop Pools

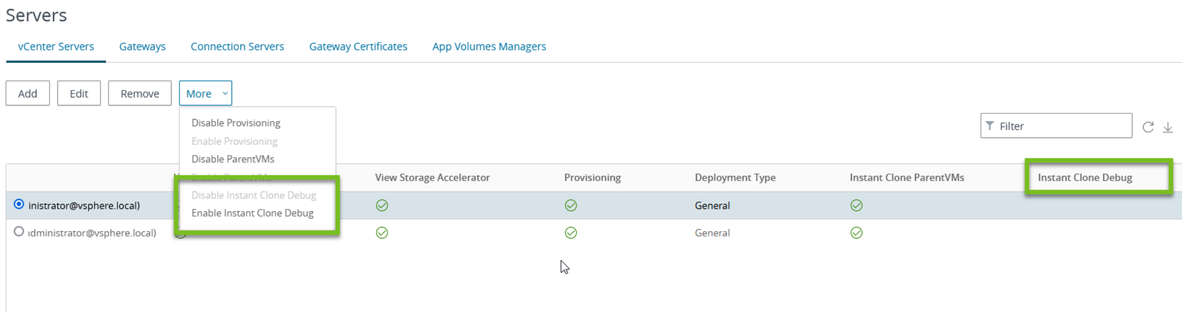
Use the Instant Clone debug mode to troubleshoot any errors that occurred when performing any desktop operations for the instant-clone desktop pools. When activated, internal virtual machines are preserved in case of an error. Administrators can then troubleshoot failed internal virtual machines.

Prerequisites

- Activate the Instant Clone Debug mode **before** creating an instant-clone desktop pool.
- Make sure that GLOBAL_CONFIG_MANAGEMENT_NOTES is configured.

Procedure

1 From the Horizon Console, select **Servers > vCenter Servers > More**.



2 From the drop-down, activate or deactivate Instant Clone Debug mode for internal virtual machines.

Option	Description
Enable Instant Clone Debug	Activating debug mode preserves Internal Template virtual machines in case of an error during pool provisioning. You can access these machines from vCenter located under [ClonePrepInternalTemplateFolder] to debug errors. These machines will not be deleted unless debug mode is turned OFF.
Disable Instant Clone Debug	Deactivating debug mode does not preserve Internal Template virtual machines in case of an error during pool provisioning. Any errored out internal template virtual machines will be deleted from vCenter under [ClonePrepInternalTemplateFolder].

Auto-debug mode is deactivated by default. It should be activated only if you see any provisioning errors to avoid preserving internal virtual machines. Once the error is resolved, auto-debug mode should be deactivated to clean up any preserved internal virtual machines.

To use the Instant Clone Debug mode effectively, activate the “Stop provisioning on error” setting to stop the priming/provisioning process at the first error. If "Stop provisioning on error" is deactivated, then the priming/provisioning process will not stop until completed.

For further debugging on instant clone actions, you can also log in to the internal VM and view the instant clone logs. See the following VMware Knowledge Base articles for further debugging on instant clone actions:

- Differences between VMware ClonePrep, QuickPrep and Microsoft Sysprep (2003797) https://kb.vmware.com/s/article/2003797
- Initial publish of an Instant Clone desktop pool image fails and the template VMs are deleted (2144938) https://kb.vmware.com/s/article/2144938
- Computer-based Global Policy Objects (GPOs) that require reboot are not applied on Instant Clones (2150495) https://kb.vmware.com/s/article/2150495
- How to change SVGA settings for Instant Clone Pools (2151745) https://kb.vmware.com/s/article/2151745

Creating Application Pools

You can give users remote access to an application by creating an application pool. Users who are entitled to an application pool can access the application remotely from a variety of client devices.

With application pools, you can deliver a single application to many users. The application runs on a farm of RDS hosts or a desktop pool. When you create an application pool, you deploy an application in the data center that users can access from anywhere on the network. An application pool has a single application and is associated with a single farm or desktop pool. To avoid errors, you must install the application on all of the RDS hosts in the farm or desktop pool.

You can select applications for an application pool in one of the following ways:

- Select from pre-installed applications
- Specify applications manually
- Select an App Volumes application for delivering published applications on demand

When you create an application pool, Horizon 8 automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all the RDS hosts in the farm or desktop pool. You can select one or more applications from the list. If you select multiple applications from the list, a separate application pool is created for each application. You can also manually specify an application that is not on the list. If an application that you want to manually specify is not already installed, Horizon 8 displays a warning message.

You cannot specify the access group in which to place the pool while creating the application pool. For published application and desktop pools, you specify the access group when you create a farm or desktop pool. An application supports the PCoIP and VMware Blast display protocols.

You can also create published applications on demand using VMware App Volumes.

Worksheet for Creating an Application Pool

When you create an application pool and manually specify an application, you can add information about the application. It is not a requirement that the application is already installed on any RDS host.

Table 15-10. Worksheet: Application Properties for Creating an Application Pool

Property	Description	Fill in Your Value Here
Select an RDS Farm or Desktop Pool	Select a farm or a desktop pool from the list provided. For desktop pools, only desktop pools with supported session type Application or Application and Desktop are available.	
ID	Unique name that identifies the pool in Horizon Console. This field is required.	
Display Name	Pool name that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as **ID**.	
Version	Version of the application.	
Publisher	Publisher of the application.	
Path	Full pathname of the application. For example, `C:\Program Files\app1.exe`. This field is required.	
Start Folder	Full pathname of the starting directory for the application.	

Table 15-10. Worksheet: Application Properties for Creating an Application Pool (continued)

Property	Description	Fill in Your Value Here
Parameters	Parameters to pass to the application when it starts. For example, you can specify `-username user1 -loglevel 3`.	
Description	Description of this application pool.	
Pre-launch	Select this option to configure an application so that an application session is launched before a user opens the application in Horizon Client. When a published application is launched, the application opens more quickly in Horizon Client. If you enable this option, the configured application session is launched before a user opens the application in Horizon Client, regardless of how the user connects to the server from Horizon Client. If you enable this option on applications published from a desktop with session type Application and Desktop, the desktop session may not be available. **Note** Application sessions can be disconnected when the **Pre-launch session timeout (applications only)** option is set when you add or edit the application farm.	
Enable single application launch limit	You can limit the number of application instances a user can launch from an application pool to just one instance. An attempt to re-launch the application will bring the first instance to focus. If you activate this setting, multi-session mode is not available.	
Connection Server Restrictions	You can restrict access to the application pool to certain Connection Servers by clicking **Browse** and selecting one or more Connection Servers. If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager application might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.	
Category Folder	Specifies the name of the category folder that contains a Start menu shortcut for the application pool entitlement on Windows client devices.	

Table 15-10. Worksheet: Application Properties for Creating an Application Pool (continued)

Property	Description	Fill in Your Value Here
Client Restrictions	Select whether to restrict access to entitled application pools from certain client computers. You must add the names of the computers that are allowed to access the application pool in an Active Directory security group. You can select this security group when you add users or groups to the application pool entitlement.	

Table 15-10. Worksheet: Application Properties for Creating an Application Pool (continued)

Property	Description	Fill in Your Value Here
Allow Machine Name Selection	Enabling this option will allow a command line launch of Horizon Client to specify a machine name to connect to, for example for test or troubleshooting purposes.	
Multi-Session Mode	You can start published application sessions in the following modes: Single-session: If the user opens a published application on client A in single-session mode, and then opens the same published application or another published application based on the same farm on client B then, the session on client A is disconnected and reconnected on client B. Multi-session: If the user opens a published application on client A in multi-session mode, and then opens the same published application or another published application based on the same farm on client B, the published application remains open on client A and a new session of the published application opens on client B. Such sessions are logged off on disconnect. You cannot enable the session pre-launch feature when multi-session mode is enabled. **Note** Multi-session mode is not available if you select **Enable application launch limit**. The multi-session mode has the following values: ■ **Disabled**. Multi-session mode is not supported. ■ **Enabled (Default Off)**. Multi-session mode is supported, but it is disabled by default. To use multi-session mode, users must enable the **Multi-Launch** setting in Horizon Client. ■ **Enabled (Default On)**. Multi-session mode is supported, and it is enabled by default. Users can disable multi-session mode by disabling the **Multi-Launch** setting in Horizon Client. ■ **Enabled (Enforced)**. Multi-session mode is always enabled. Users cannot disable it in any version of Horizon Client and the application is always launched in multi-session mode.	

Table 15-10. Worksheet: Application Properties for Creating an Application Pool (continued)

Property	Description	Fill in Your Value Here
	When multi-session mode is enabled you can also configure the **max-sessions count** setting. This sets the maximum number of concurrent multi-sessions that can be started by a user for the same published application from different client devices. You can open a published application from a client in both the single-session mode and multi-session mode, which is based on the multi-session mode configuration. In this case, the client has one single-session and one multi-session. Enabling multi-session mode affects how HTML Access behaves when it is started from Workspace ONE. For more information, see the Workspace ONE documentation. For more information about using the **Multi-Launch** setting, see the Horizon Client documentation. **Note** This setting is not supported for applications based on a desktop pool.	

Create an Application Pool

You create an application pool as part of the process to give users access to an application that runs on RDS hosts or a desktop pool.

Prerequisites

- Set up RDS hosts. See Setting Up Remote Desktop Services Hosts.
- Create a farm that contains the RDS hosts. See Creating and Managing Farms.
- If you plan to add the application pool manually, gather information about the application. See Worksheet for Creating an Application Pool

Procedure

1 In Horizon Console, select **Inventory > Applications**.

2 Click **Add**.

3 Specify whether you want to add the pool manually, add it from installed applications, or add it from an App Volumes Manager.

   If you choose to add an application pool manually, use the configuration information you gathered in the worksheet. If you select applications from the list that Horizon Console displays, you can select multiple applications. A separate pool is created for each application.

What to do next

Entitle users to access the pool. You can also view the number of entitled users that are using a published application in the **User Count** column in the application pools page.

If you need to ensure that Connection Server launches the application only on RDS hosts that have sufficient resources to run the application, configure an anti-affinity rule for the application pool.

Note For applications running on desktop pools, the anti-affinity rule is supported only for applications created from floating desktop pools, and not from dedicated desktop pools.

See Configure an Anti-Affinity Rule for an Application Pool in Horizon Console.

If you have connected your pod to Horizon Cloud and want information on configuring published desktop pools for use in a Universal Broker environment, see Horizon Pods - Configure RDSH Desktops and Applications for a Universal Broker Environment.

Managing Application Pools

You can add, edit, delete, or entitle application pools in Horizon Console.

Edit an Application Pool

You can edit an existing application pool to configure settings such as display name, version, publisher, path, start folder, parameters, and description. You cannot change the ID or access group of an application pool.

Prerequisites

- Familiarize yourself with the settings of an application pool.
- You might need to configure an anti-affinity rule to ensure that Connection Server launches the application only on RDS hosts that have sufficient resources to run the application.

Procedure

1 In Horizon Console, select **Inventory > Applications**.

2 Select a pool and click **Edit**.

3 Make changes to the pool settings.

4 Click **OK**.

Delete an Application Pool

When you delete an application pool, users can no longer launch the application in the pool.

You can delete an application pool even if users are currently accessing the application. After the users close the application, they can no longer access the application.

Procedure

1. In Horizon Console, select **Inventory** > **Applications**.
2. Select one or more application pools and click **Delete**.
3. Click **OK** to confirm.

Duplicate an Application Pool

You can duplicate an application pool to create multiple applications that are similar to each other.

When you duplicate an application pool, you can change the application pool ID and description to create a new application pool.

Note If there is an icon for the original application pool, the icon does not get associated with the duplicate application pool. However, you can assign the original icon to the duplicate application pool.

Note If there are user entitlements for the original application pool, the duplicate application pool does not get these entitlements and you must entitle users to the duplicate application pool again.

Procedure

1. In Horizon Console, select **Inventory** > **Applications**.
2. Select an application pools and click **Duplicate**.
3. Enter an application pool ID.
4. (Optional) Enter a display name and a description.
5. Click **OK**.

What to do next

Entitle users to the duplicate application pool. See "Entitling Users and Groups" in the *Horizon 8 Administration* document.

Change the Icon of a Published Application

You can customize the icons for published applications for end users. When you change the icon for a published application, the new application icon is available for the end user to view on the published desktop.

Prerequisites

- Verify that the icon is available in a 32-bit .PNG file format.

Procedure

1. In Horizon Console, select **Inventory** > **Applications**.

2. Select an application pool or multiple application pools and click **Application Icon > Associate Application Icon**.
3. To upload an icon, click **Upload Icon File** and browse for an icon in the .PNG format.

   The icon file must be between 16x16 pixels and 256x256 pixels.
4. Click **OK**.

Results

The icon appears for the published application on the published desktop.

Remove the Icon of a Published Application

You can remove the icon of a published application to replace it with another icon. When you remove the icon for a published application, the published application is replaced with the default icon on the published desktop. You can remove icons from multiple published applications only if all published applications have the same icon. You cannot select multiple published applications that have different icons to remove an icon.

Procedure

1. In Horizon Console, select **Inventory > Applications**.
2. Select an application pool or multiple application pools and click **Application Icon > Remove Application Icon**.

Results

The published application is replaced with the default icon on the published desktop.

Enable or Disable an Application Pool

When you enable an application pool, entitled users have access to the application pool. When you disable an application pool, entitled users no longer have access to the application pool. You can enable or disable one or multiple application pools.

Prerequisites

- Verify that you have the **Enable Farms, Desktops and Applications Pools** privilege.

Procedure

1. In Horizon Console, select **Inventory > Applications**.
2. Select one or more application pools.
3. Choose to enable or disable an application pool or pools.
   - To enable an application pool or pools, click **More > Enable Pool**.
   - To disable an application pool or pools, click **More > Disable Pool**.
4. Click **OK** to confirm.

Configure an Anti-Affinity Rule for an Application Pool in Horizon Console

When you configure an anti-affinity rule for an application pool, Horizon Connection Server attempts to launch the application only on RDS hosts that have sufficient resources to run the application. This feature can be useful for controlling applications that consume large amounts of CPU or memory resources.

An anti-affinity rule consists of an application matching pattern and a maximum count. For example, the application matching pattern might be `autocad.exe` and the maximum count might be 2.

Connection Server sends the anti-affinity rule to Horizon Agent on an RDS host. If any applications running on the RDS host have process names that match the application matching pattern, Horizon Agent counts the current number of instances of those applications and compares the number to the maximum count. If the maximum count is exceeded, Connection Server skips that RDS host when it selects an RDS host to run new sessions of the application.

Prerequisites

- Create the application pool. See Create an Application Pool.
- Become familiar with the constraints of the anti-affinity feature. See Anti-Affinity Feature Constraints.

Procedure

1. In Horizon Console, select **Inventory > Applications**.
2. Select the pool to modify and click **Edit**.
3. In the **Anti-Affinity Patterns** text box, type a comma-separated list of patterns to match against the process names of other applications running on RDS hosts.

   The pattern string can include the asterisk (*) and question mark (?) wildcard characters. An asterisk matches zero or more characters and a question mark matches any single character. For example, **`*pad.exe,*notepad.???`** matches `wordpad.exe`, `notepad.exe`, and `notepad.bat`, but it does not match `wordpad.bat` or `notepad.script`.

   Note Horizon 8 counts multiple patterns that match for an application in a single session as a single match.

4. In the **Anti-Affinity Count** text box, type the maximum number of other applications that can be running on the RDS host before the RDS host is rejected for new application sessions.

   The maximum count can be an integer from 1 to 20.

5. Click **Submit** to save your changes.

Anti-Affinity Feature Constraints

The anti-affinity feature has certain constraints.

- Anti-affinity rules affect new application sessions only. An RDS host that contains sessions in which a user has previously run an application is always reused for the same application. This behavior overrides reported load preferences and anti-affinity rules.
- Anti-affinity rules do not affect application launches from within an RDS desktop session.
- RDS session limits prevent application sessions from being created, regardless of anti-affinity rules.
- In certain circumstances, the instances of applications on the RDS host might not be restricted to the maximum count that you specify. For example, Horizon 8 cannot determine the exact instance count if other applications for other pending sessions are in the process of being launched.
- Inter-application anti-affinity rules are not supported. For example, large application classes, such as Autocad and Visual Studio instances, cannot be counted in a single rule.
- Do not use anti-affinity rules in environments where end-users use Horizon Client on mobile clients. Anti-affinity rules can result in multiple sessions in the same farm for an end user. Reconnecting to multiple sessions on mobile clients can result in indeterminate behavior.
- Anti-Affinity rules consider only the connected number of sessions for load balancing. However, load balancing for RDS hosts considers the sum of the connected, pending, and disconnected sessions for load balancing.

Setting up Published Applications on Demand

You can create published applications on demand using VMware App Volumes. Published applications on demand helps reduce the number of OS images and RDS farms. With the addition of App Volumes, Horizon 8 can configure individual RDS hosts for logged in users. This consolidates RDS farms based on real-time need, and enables you to easily manage multi-farm environments and simplify the lifecycle management of the applications.

To access published applications on demand, you add one or more VMware App Volumes Managers to Horizon Console, associate it with a farm, select applications and add user and group entitlement. These tasks need to be performed in the order in which they are documented.

Prerequisites

- The following minimum product versions are required for this feature:
  - Horizon Agent 2212
  - VMware App Volumes 4, version 2212
- Install and configure an App Volumes Manager and note the FQDN or IP address, port, user name, and password.
- Ensure that the App Volumes Manager is configured with a self-signed SSL certificate.

- Ensure you have at least one application package imported to the App Volumes Manager and assigned the `CURRENT` marker. All packages used for published applications on demand must be assigned the `CURRENT` marker.
- In the App Volumes Manager advanced settings, activate the option **Allow package delivery to any operating system**. For more information, see *App Volumes Manager Configuration Settings Page* in the App Volumes documentation.
- Ensure that you have at least one automated RDS farm in your environment. For more information, see Creating and Managing Farms.
- Ensure that the golden image used to create the farm has both Horizon Agent and the App Volumes agent installed. See the App Volumes documentation for details.

  Note Create RDS farms using a golden image that has Windows Update disabled. Apply Windows Updates by updating the golden image and scheduling maintenance for the farm to apply the new golden image.

Procedure

1. Add a VMware App Volumes Manager.
2. Associate App Volumes Manager with a Farm.
3. Add Applications.

Add a VMware App Volumes Manager

If you want to deliver published applications on demand with Horizon 8, add the App Volumes Manager from where you want to access the applications to Horizon Console. After you associate a farm with the App Volumes Manager, any host in the farm can access the applications on the App Volumes Manager. The App Volumes agent installed on the RDS hosts in the farm must be configured to reference this App Volumes Manager instance.

A default self-signed certificate is installed when you install App Volumes Manager. VMware Horizon Connection Server uses SSL to communicate with the App Volumes Manager and validate the certificate. Administrators have the option to accept the SSL Certificate Thumbprint when adding or editing an App Volumes Manager. For more information, see Managing SSL Between App Volumes Manager and Agent in the *VMware App Volumes Administration Guide*.

Depending on your environment and setup, add all App Volumes Managers that you want to be associated with Connection Server and used with published apps on demand. You can add individual App Volumes Managers, which would be multiple records if you have different App Volumes Managers that you want to use for published apps on demand, or add a load balancer which would only have one record.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. Click the **App Volumes Managers** tab.

3 Click **Add**.

4 Add the App Volumes Manager FQDN or IP address, port, and user name and password.

   You can specify a load balancer IP address.

5 Click **OK**.

   The App Volumes Manager certificate validation occurs.

6 If you see a message indicating an invalid certificate, click **View Certificate**.

   The certificate information is displayed.

7 Click **Accept** to trust the SSL Certificate based on the Thumbprint.

   The App Volumes Manager is added in Connection Server.

8 To verify the validation, select **Settings > Servers**.

9 Click the **App Volumes Managers** tab.

10 Click **Certificate** and select **Re-Validate Certificate**.

Results

The App Volumes Manager is added to Horizon Console and the SSL certificate is pushed to Horizon Connection Server.

Associate App Volumes Manager with a Farm

For published applications on demand, you must associate an App Volumes Manager with an automated instant-clone farm. Applications on the App Volumes Manager can be published from any host on that farm.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Select the farm you want to associate and click **More Commands > Associate App Volumes Manager**.

3 Select the App Volumes Manager that manages the farm and click **OK**.

Add Applications

To deliver applications on demand, you must add applications from the App Volumes Manager and give users access to those applications.

Procedure

1 In Horizon Console, select **Inventory > Applications**.

2 Click **Add > Add from App Volumes Manager** and select a farm.

   All applications on the App Volumes Manager associated with the selected farm are displayed.

3 Select applications and click **Next**.

4 Edit the ID and display names of the selected applications as appropriate and click **Submit**.

5 Follow the prompts on the wizard to select users and groups that can access the selected applications and click **OK**.

   The applications are added to the Application Pool table.

What to do next

Monitor the health of the App Volumes Manager by navigating to **Monitor > Dashboard > View** and clicking the App Volumes tab.

Manage App Volumes Managers

You can edit, delete, or unassociate an App Volumes Manager. You can also manually push an App Volumes Manager certificate to the Connection Server.

Edit App Volumes Manager

You can edit the server address, port, user name, or password of an App Volumes Manager.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 Click the App Volumes Managers tab.

3 Select an App Volumes Manager and click **Edit**.

4 Edit the information as appropriate and click **OK**.

Delete an App Volumes Manager

You can delete an App Volumes Manager from the Horizon Console.

Prerequisites

Delete the associations between the App Volumes Manager to be deleted and farms.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 Click the App Volumes Managers tab.

3 Select an App Volumes Manager and click **Delete**.

Unassociate App Volumes Manager

You can unassociate an App Volumes Manager from a farm after deleting all application pools from that farm.

Prerequisites

Delete the applications published from the App Volumes Manager.

Procedure

1 In Horizon Console, navigate to **Inventory > Farms** and select a farm

2 Click **More Commands > Unassociate App Volumes Manager** and click **OK**.

Results

The App Volumes Manager's farm association is removed from the Horizon Console.

Push Certificate To App Volumes Manager

When you add an App Volumes Manager, Horizon Console pushes the SSL certificate which is used to verify application entitlements in App Volumes Manager. In case there is an error during launch due to entitlement, you can push the certificate manually.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 Click the App Volumes Managers tab.

3 Select an App Volumes Manager and click **Push Certificate**.

4 In the Push Certificate dialog box, click **OK**.

Revalidate App Volumes Manager Certificate

You can revalidate the App Volumes Manager certificate for an already added App Volumes Manager.

In some cases, an already added App Volumes Manager can change its certificate, resulting in a broken connection between Horizon Connection Server and the App Volumes Manager. To restore the connection, perform a certificate revalidation.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 Click the **App Volumes Managers** tab.

3 Click **Certificate** and select **Re-Validate Certificate**.

Results

The App Volumes Manager SSL certificate is pushed to Horizon Connection Server.

Managing RDS Hosts and Sessions

In Horizon Console, you can perform management operations such as configuring or deleting RDS hosts or manage sessions for published desktops and applications.

Managing RDS Hosts in Horizon Console

You can perform certain management tasks on the manual or automated farm of RDS hosts you have created. Note that some tasks are applicable to both manual and automated farms, whereas others are only applicable to one type of farm.

When you manually set up an RDS host, it automatically registers with Horizon Connection Server. You cannot separately register an RDS host with Connection Server. For a manual farm, you can perform the following management tasks:

- Edit the RDS host.
- Add the RDS host to a manual farm.
- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

For an automated farm of RDS hosts, you can perform the following management tasks:

- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

Edit an RDS Host in a Manual Farm

You can change the number of connections that an RDS host can support. You can set it to any positive number, or to unlimited.

You can only edit an RDS host that you set up manually, but not an RDS host that is in an automated farm.

Procedure

1. In Horizon Console, select **Settings > Registered Machines**.
2. Select an RDS host and click **Edit**.
3. Specify a value for the setting **Number of connections**.
4. Click **OK**.

Add an RDS Host to a Manual Farm

You can add an RDS host that you set up manually to a manual farm to increase the scale of the farm or for other reasons. You can only add RDS hosts to a manual farm.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Click the farm ID.
3. Select the **RDS Hosts** tab.

4 Click **Add**.

5 Select one or more RDS hosts.

6 Click **OK**.

Remove an RDS Host from a Manual or Automated Farm

You can remove an RDS host from a manual farm to reduce the scale of the farm, to perform maintenance on the RDS host, or for other reasons. As a best practice, disable the RDS host and ensure that users are logged off from active sessions before you remove a host from a farm.

If users have application or desktop sessions on hosts that you remove, the sessions remain active, but Horizon 8 does not track them. A user who disconnects from a session will be unable to reconnect to it, and any unsaved data might be lost.

You can also remove an RDS host from an automated farm. One possible reason might be that the RDS host is in an unrecoverable error state.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Click the farm ID.

3 Select the **RDS Hosts** tab.

4 Select one or more RDS hosts.

5 Click **Remove from farm**.

6 Click **OK**.

Remove a Registered RDS Host from Horizon

You can remove from Horizon 8 an RDS host that you set up manually and that you no longer plan to use. The RDS host must not currently be in a manual farm.

Prerequisites

Verify that the RDS host does not belong to a farm.

Procedure

1 In Horizon Console, select **Settings > Registered Machines**.

2 Select an RDS host and click **Remove**.

3 Click **OK**.

Results

After you remove an RDS host, to use it again, you must reinstall Horizon Agent.

Disable or Enable an RDS Host in a Manual or Automated Farm

When you disable an RDS host, Horizon 8 no longer uses it to host new published desktops or applications. Users can continue to use published desktops and applications that are currently open.

Procedure

1. In Horizon Console, select **Inventory > Farms**.
2. Click the farm ID.
3. Select the **RDS Hosts** tab.
4. Select an RDS host and click **More Commands**.
5. Click **Enable** or **Disable**.
6. Click **OK**.

Results

If you enable the RDS host, a check mark appears in the Enabled column, and Available appears in the Status column. If you disable the RDS host, the Enabled column is empty and Disabled appears in the Status column.

Status of RDS Hosts in Horizon Console

An RDS host can be in various states from the time that it is initialized. As a best practice, check that RDS hosts are in the state that you expect them to be in before and after you perform tasks or operations on them.

Table 15-11. Status of an RDS Host

Status	Description
Startup	Horizon Agent has started on the RDS host, but other required services such as the display protocol are still starting. The agent startup period also allows other processes such as protocol services to start up.
Disable in progress	RDS host is in the process of being disabled while sessions are still running on the host. When the sessions end, the status changes to Disabled.
Disabled	Process of disabling the RDS host is complete.
Validating	Occurs after Connection Server first becomes aware of the RDS host, typically after Connection Server is started or restarted, and before the first successful communication with Horizon Agent on the RDS host. Typically, this state is transient. This state is not the same as the Agent unreachable state, which indicates a communication problem.
Agent disabled	Occurs if Connection Server disables Horizon Agent. This state ensures that a new desktop or application session cannot be started on the RDS host.
Agent unreachable	Connection Server cannot establish communication with Horizon Agent on an RDS host.
Invalid IP	Subnet mask registry setting is configured on the RDS host, and no active network adapters have an IP address within the configured range.

Table 15-11. Status of an RDS Host (continued)

Status	Description
Agent needs reboot	Component was upgraded, and the RDS host must be restarted to allow Horizon Agent to operate with the upgraded component.
Protocol failure	The RDP display protocol is not running correctly. If RDP is not running and PCoIP is running, clients cannot connect using either RDP or PCoIP. However, if RDP is running and PCoIP is not running, clients can connect using RDP.
Domain failure	RDS host encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Configuration error	RDS role is not enabled on the server.
Unknown	RDS host is in an unknown state.
Available	RDS host is available. If the host is in a farm, and the farm is associated with a published desktop or application pool, it will be used to deliver published desktops or applications to users.
Drain	RDS host is in drain mode and not accepting new connections.
Drain mode until restart	RDS host is in drain mode and not accepting new connections until it is restarted.

Monitor RDS Hosts in Horizon Console

You can monitor the status and view the properties of RDS hosts in both manual and automated farms in Horizon Console.

Procedure

◆ In Horizon Console, navigate to the page that displays the properties that you want to view.

Properties	Action
DNS Name, Type, Image, Pending Image, Task, Max Number of Connections, Sessions, Agent Version, Enabled, Status	■ In Horizon Console, select **Inventory > Farms**. ■ Select a farm and click the **RDS Hosts** tab.
RDS Host, Farm, Desktop Pool, Agent Version, Sessions, Status	■ In Horizon Console, select **Inventory > Machines**. ■ Click the **RDS Hosts** tab.
DNS Name, Type, RDS Farm, Max Number of Connections, Sessions, Agent Version, Enabled, Status	■ In Horizon Console, select **Settings > Registered Machines**. ■ Click the **RDS Hosts** tab.

Results

The properties are displayed and have the following meanings:

Property	Description
RDS Host	Name of the RDS host.
Farm	Farm to which the RDS host belongs.
Desktop Pool	Published desktop pool associated with the farm.
Agent Version	Version of Horizon Agent that runs on the RDS host.
Sessions	Number of client sessions.
DNS Name	DNS name of the RDS host.
Type	Version of Windows Server that runs on the RDS host.
RDS Farm	Farm to which the RDS host belongs.
Image	Image of the RDS host on the farm.
Pending Image	Pending image of the RDS host on the farm.
Task	Task being performed on the RDS host of the farm.
Max Number of Connections	Maximum number of connections that the RDS host can support.
Enabled	Whether the RDS host is enabled.
Status	State of the RDS host. See Status of RDS Hosts in Horizon Console for a description of the possible states.

Manage Published Desktop and Application Sessions in Horizon Console

When a user launches a published desktop or application, a session is created. You can disconnect and log off sessions, send messages to clients, reset, and restart virtual machines.

Procedure

1 In Horizon Console, navigate to where session information is displayed.

Session Type	Navigation
Remote desktop sessions	Select **Inventory > Desktops**, click a pool's ID, and click the **Sessions** tab. The **Sessions** column also appears on the **Desktop Pools** page for all desktops. Select **Inventory > Farms**, click a farm's ID, and click the **Sessions** tab. You can also view the published applications associated with a session. The **Application Names** column displays the published applications associated with a session. The **Sessions** column also appears on the **Farms** page for all farms. Select **Settings > Registered Machines**, and view the **Sessions** column.
Remote desktop and application sessions	Select **Monitor > Sessions**.
Sessions associated with a user or user group	■ Select **Users and Groups**. ■ Click a user's name or a user group's name. ■ Click on the **Sessions** tab.

2 Select a session.

To send a message to users, you can select multiple sessions. You can perform the other operations on only one session at a time. You can perform a log off operation only on a session that is not connected from a vSphere console.

3 Choose whether to disconnect, log off, send a message, restart a desktop, or reset a virtual machine.

Option	Description
Disconnect Session	Disconnects the user from the session.
Logoff Session	Logs the user off the session. Data that is not saved is lost.
Send Message	Send a message to Horizon Client. You can label the message as **Info**, **Warning**, or **Error**.
Restart Desktop	Performs a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine. **Note** This option is not available for instant-clone farms.
Reset Virtual Machine	Performs a reset operation on a virtual machine without the graceful operating system restart, which performs a hard power-off and power-on of the virtual machine. **Note** This option is not available for instant-clone farms.

4 Click **OK**.

Results

The session properties have the following descriptions:

Property	Description
RDS Host	Name of the RDS host.
Farm	Farm to which the RDS host belongs.
Desktop Pool	RDS desktop pool associated with the farm.
Agent Version	Version of Horizon Agent that runs on the RDS host.
Sessions	Number of client sessions.
DNS Name	DNS name of the RDS host.
Type	Version of Windows Server that runs on the RDS host.
Client ID	Name or the MAC address of the client.
Client Version	Version of Horizon Client for the user's session.
RDS Farm	Farm to which the RDS host belongs.
Max Number of Connections	Maximum number of connections that the RDS host can support.
Enabled	Whether the RDS host is enabled.
Status	State of the RDS host. See Status of RDS Hosts in Horizon Console for a description of the possible states.

Configuring Load Balancing for RDS Hosts in Horizon Console

You can configure load balancing for RDS hosts by configuring load balancing settings in Horizon Console or by creating and configuring load balancing scripts.

By default, Connection Server uses the RDS hosts load index to balance the placement of desktop and application sessions.

Load Balancing Settings in Horizon Console

Horizon calculates the Server Load Index based on the load balancing settings you configure in Horizon Console. The Server Load Index indicates the load on the server. The Server Load Index can range from 0 to 100, where 0 represents no load and 100 represents full load. A Server Load Index of -1 indicates that load balancing is disabled. You can view the Server Load Index in the Horizon Console dashboard. Horizon also offers threshold values in the load balancing settings for logon storm handling. See Load Balancing Settings.

Load Balancing Scripts

You can also override the default behavior of the load balancing settings and control the placement of new published desktop and application sessions by writing and configuring load balancing scripts.

You can write your own custom load balancing scripts, or you can use one of the sample load balancing scripts provided with Horizon Agent. To use custom load balancing scripts, you must select the **Use Custom Script** load balancing setting in Horizon Console.

You can run these scripts on your own schedule or run these scripts with Horizon 8. For more information on configuring load balancing scripts in Horizon 8, see Configure a Load Balancing Script on an RDS Host.

Configuring load balancing scripts involves enabling the VMware Horizon View Script Host service and setting a registry key on each RDS host in a farm.

Load balancing scripts must write the load index to the `CustomLoadValue` registry key with the `REG_DWORD` registry setting in the following location:

```
HKLM\Software\VMware, Inc.\VMware VDM\Performance Stats\CustomLoadValue
```

The value must be between 0-100.

Horizon 8 calculates the raw performance metrics that are written to the `Performance Stats` registry key in the following location:

```
HKLM\Software\VMware, Inc.\VMware VDM\Performance Stats
```

You can use the raw performance metrics and combine these with your custom index factor for writing custom scripts.

Configure Load Balancing Settings on an RDS Host in Horizon Console

You can configure load balancing settings in Connection Server to control the placement of published desktop and application sessions on RDS hosts.

Procedure

1 In Horizon Console, select **Inventory > Farms**.

2 Click **Add** and follow the prompts to the **Load Balancing Settings** page.

3 Configure the load balancing settings. See, Load Balancing Settings.

4 Follow the prompts to complete the wizard and click **Submit**.

Load Balancing Settings

Horizon 8 calculates the Server Load Index based on the load balancing settings you configure in Horizon Console. The Server Load Index indicates the load on the server. The Server Load Index can range from 0 to 100, where 0 represents no load and 100 represents full load. A Server Load Index of -1 indicates that load balancing is disabled. You can view the Server Load Index in the Horizon Console dashboard. Horizon also offers threshold values in the load balancing settings for logon storm handling.

Logon storms occur when a large number of users log into the farm within a short time interval. In these events, the Server Load Index reported by the RDS hosts may be stale, or out of date, because the sampling interval for the CPU, Memory, and Disk statistics is 30 seconds and only updates those metrics after 30 seconds.

RDS session load balancing mitigates flooding the least loaded RDS host with all the start sessions during a logon storm by classifying RDS hosts into three distinct groups and ensuring session requests are evenly distributed among all the RDS hosts to prevent overwhelming the least loaded RDS host during a logon storm.

Horizon Connection Server categorizes RDS hosts into three buckets:

1. RDS hosts that support all default functionalities, such as multisession, unauthenticated access, and RDP/PCOIP/BLAST protocols. These agents must have a load index less than the configured Load Index Threshold or `pae-RDSLoadIndexThreshold` value (the default value is 20) and fewer connecting sessions than the Connecting Session Threshold or `pae-RDSConnectingSessionThreshold` value (the default value is 20). If there are fewer than the minimum configured RDS agents or `pae-MinRDSServersInLBQueue` (the default value is 4), the load index threshold is dynamically increased until the minimum number of RDS agents is attained.
2. RDS hosts that support non-default functionalities. These agents must have a load index less than the configured Load Index Threshold value and fewer connecting sessions than the Connecting Session Threshold.
3. RDS servers with a load index value greater than the configured Load Index Threshold value or pending sessions greater than the Connecting Session Threshold. If no servers are available in the first or second bucket, Connection Server then chooses an RDS host from this bucket.

When Connection Server receives a start session request, it selects an RDS host from either the first or second bucket based on the session request. The distribution of start session requests among RDS hosts in the first bucket is done fairly where each RDS host receives an equal share, ensuring all hosts in the first bucket are treated equally in terms of session allocation.

You can configure load balancing settings in Horizon Console: `Load Index Threshold` and `Connecting Session Threshold` values are used solely by the RDS host to reject and redirect sessions based on the number of concurrently connecting sessions on the machine and the load index by using threshold values configured in Horizon Console.

You can also configure load balancing settings using ADAM attributes: `pae-RDSLoadIndexThreshold`, `pae-RDSConnectingSessionThreshold`, and `pae-MinRDSServersInLBQueue` are used solely by Connection Server for fair distribution of sessions among RDS hosts.

You can also configure load balancing settings on each RDS host through Agent Configuration Policy Settings. For more information, see "VMware View Agent Configuration ADMX Template Settings" in the *Horizon Remote Desktop Features and GPOs* document. If both policy settings and Horizon Console settings for logon storm handling thresholds are set, the policy settings will take precedence.

Table 15-12. Load Balancing Settings in Horizon Console

Option	Description
Use custom script	Select this setting to use a custom script for load balancing. If this setting is enabled, Horizon 8 does not consider other load balancing metrics for calculating server load index, but it will consider the Connecting Session Threshold and Load Index Threshold used for logon storm handling. To get the server load index, Horizon reads the `CustomLoadValue` registry key in the following location: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. See Writing a Load Balancing Script for an RDS Host.
Include session count	Select this setting to include the session count on the RDS host for load balancing. If none of the settings are selected for load balancing and if the custom script setting is not selected, Horizon 8 uses the session count by default. Disable this setting if you do not need to consider the session count for load balancing.
CPU usage threshold	Threshold value for the CPU usage in percentage. Horizon 8 uses the configured CPU threshold to calculate the CPU load index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.
Memory usage threshold	Threshold value for the memory in percentage. Horizon 8 uses the configured memory threshold to calculate the Memory Load Index factor. You can set a value from 0 to 100. The recommended value is 90. By default, this setting is not considered for load balancing. The default value is 0.
Disk queue length threshold	Threshold of the average number of both read and write requests that were queued for the selected disk during the sample interval. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing.
Disk read latency threshold	Threshold of the average time of read of data from the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.
Disk write latency threshold	Threshold of the average time of write of data to the disk in milliseconds. Horizon 8 uses the configured threshold to calculate the Disk Load Index factor. You can set the value to any positive integer. By default, this setting is not considered for load balancing. The default value is 0.
Connecting session threshold	Threshold value for connecting sessions, for use in logon storm handling. The configured threshold specifies the maximum number of sessions that can concurrently log into each RDSH agent machine in the farm, exempting reconnecting sessions. This is configurable from 0 to 150. The recommended value is 20, but the value can be lowered to decrease the number of concurrent sessions that can log in to further protect each RDS host. By default, this threshold is disabled and does not deny session logons (default value is 0).
Load index threshold	Threshold value for load index, for use in logon storm handling. The configured threshold specifies the minimum load index at which each RDSH agent machine in the farm will start denying session logins, exempting reconnecting sessions. This is configurable from 0 to 100. The recommended value is 0 (disabled). The value can be set to a higher number (between 90-100) to reject sessions on an RDS host based on an exceedingly high load index. By default, this threshold is disabled and does not deny session logons (default value is 0).

Writing a Load Balancing Script for an RDS Host

You can write a load balancing script to generate a load value based on any RDS host metric that you want to use for load balancing.

Your load balancing script must write the load index value to the `CustomLoadValue` registry key in the following location: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. This value must be between 0-100.

If at least one RDS host in the farm returns a valid load value, the Connection Server assumes a load value of 25 for the other RDS hosts in farm until their load balancing scripts return valid values. If no RDS host in the farm returns a valid load value, the load balancing feature is disabled for the farm.

Note The Horizon Console dashboard shows -1 for those RDS hosts that do not report a load index. Connection Server only uses the value of 25 for internal load balancing logic.

If your load balancing script writes an invalid load value to the `CustomLoadValue` registry key, the value is capped at 100 and returned as the load index to the Connection Server. If the script is unable to create the `CustomLoadValue` registry key, the default value of 0 is sent as the load index to the Connection Server. If the custom script does not finish running within 10 seconds, Horizon 8 terminates the script after 10 seconds and uses stale values from the `CustomLoadValue` registry key as the load index.

Copy your load balancing script to the Horizon Agent `scripts` directory (`C:\Program Files\VMware\VMware View\Agent\scripts`) on each RDS host in the farm. You must copy the same script to every RDS host in the farm.

For an example how to write a load balancing script, see the sample scripts in the Horizon Agent `scripts` directory. For more information, see Sample Load Balancing Scripts for RDS Hosts.

Sample Load Balancing Scripts for RDS Hosts

When you install Horizon Agent on an RDS host, the installer places sample load balancing scripts in the Horizon Agent `scripts` directory (`C:\Program Files\VMware\VMware View\Agent\scripts`).

Table 15-13. Sample Load Balancing Scripts

Name	Description
`cpuutilisation.vbs`	Reads the percentage of CPU that has been utilized from the registry and writes it to the `CustomLoadValue` registry key.
`memoryutilisation.vbs`	Reads the percentage of memory that has been utilized from the registry and writes it to the `CustomLoadValue` registry key.

Enable the VMware Horizon View Script Host Service on an RDS Host

You must enable the VMware Horizon View Script Host service on an RDS host before you configure a load balancing script. The VMware Horizon View Script Host service is disabled by default.

Procedure

1. Log in to the RDS host as an administrator.
2. Start Server Manager.
3. Select **Tools > Services** and navigate to the VMware Horizon View Script Host service.
4. Right-click **VMware Horizon View Script Host** and select **Properties**.
5. In the Properties dialog box, select **Automatic** from the **Startup type** drop-down menu and click **OK** to save your changes.
6. Right-click **VMware Horizon View Script Host** and select **Start** to start the VMware Horizon View Script Host service.

Results

The VMware Horizon View Script Host service restarts automatically each time the RDS host starts.

What to do next

Configure your load balancing script on each RDS host in the farm. See Configure a Load Balancing Script on an RDS Host.

Configure a Load Balancing Script on an RDS Host

You must configure the same load balancing script on every RDS host in the farm. Configuring a load balancing script involves setting a registry key on the RDS host.

If you are using an automated farm, you perform this procedure on the golden image virtual machine for the automated farm.

Important You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm. If you configure a load balancing script on only some of the RDS hosts in a farm, Horizon Console sets the status of the farm to red.

Prerequisites

- Write a load balancing script and copy the same script to the Horizon Agent `scripts` directory on each RDS host in the farm. See Writing a Load Balancing Script for an RDS Host.
- Enable the VMware Horizon View Script Host service on the RDS host. See Enable the VMware Horizon View Script Host Service on an RDS Host.

Procedure

1 Log in to the RDS host as an administrator.

2 Start Server Manager.

3 Select **Tools > System Configuration**, click the **Tools** tab, and launch the Registry Editor.

4 In the registry, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.

5 In the navigation area, select the **RdshLoad** key.

The values for the **RdshLoad** key, if any, appear in the topic area (the right pane).

6 Right-click in the topic area for the **RdshLoad** key, select **New > String Value**, and create a new string value.

As a best practice, use a name that represents the load balancing script to be run, for example, **`cpuutilisationScript`** for the `cpuutilisation.vbs` script.

7 Right-click the entry for the new string value you created and select **Modify**.

8 In the **Value data** text box, type the command line that invokes your load balancing script and click **OK**.

Type the full path to your load balancing script.

For example: `cscript.exe "C:\Program Files\VMware\VMware View Agent\scripts\cpuutilisation.vbs"`

9 Restart the Horizon Agent service on the RDS host to make your changes take effect.

Results

Your load balancing script begins to run on the RDS host.

What to do next

Repeat this procedure on each RDS host in the farm. If you performed this procedure on the golden image virtual machine for an automated farm, provision the automated farm.

To verify that your load balancing script is working correctly, see Verify a Load Balancing Script.

Verify a Load Balancing Script

You can verify that your load balancing script is working correctly by viewing RDS farm and RDS host information in Horizon Console.

Procedure

1 In Horizon Console, navigate to **Monitor > Dashboard**.

2 In the **Issues** pane, click **View**.

3 Click **RDS Farms** and click the name of each RDS host to view its load index.

The Server load field in the details dialog box shows the server load index reported by Horizon Agent. The value should be between 0-100.

The status of the farm should be green. If a load balancing script is configured on only some of the RDS hosts in a farm, Horizon Console sets the status of the farm to yellow. You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm.

What to do next

If load balancing is not working as you expected, verify the content of your load balancing script. If the script is written correctly, it should update the `CustomLoadValue` registry key on Horizon Agent with the expected load index. The `CustomLoadValue` registry key is located in the following location: `HKLM\Sofware\VMware Inc.\VMware VDM\Performance Stats\CustomLoadValue`. Verify that this registry key is updated correctly. If you use Horizon 8 to run your scripts, verify that the VMware Horizon View Script Host service is running. Also, verify that the same load balancing script is configured on each RDS host in the farm.